Informations- und Kommunikationstechnologien – Katalysator der Transformation im Bereich Verteidigung

BITKOM
Connecting visions - creating solutions

Impressum

Herausgeber:
BITKOM
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin-Mitte

Telefon 030/27576-0
Telefax 030/27576-400

bitkom@bitkom.org
www.bitkom.org

Autorenteam:
Arbeitskreis Verteidigung

Gestaltung:
PROFORMA

V. i. S. d. P.:
Dr. Bernhard Rohleder

Ansprechpartner:
Fabian Bahr
Telefon: 030/27576-102
Fax: 030/27576-400
f.bahr@bitkom.org

Inhalt

Geleitwort

Jörg Menno Harms
Vizepräsident BITKOM

Die erzielten Fortschritte beim Modernisierungsprozess der Bundeswehr sind evident. Potenzial besteht insbesondere beim verstärkten Einsatz von Informations- und Kommunikationstechnologien (ITK) im Rahmen der Transformation der Bundeswehr. In der Publikation „Ohne NC kein W“ wies der Arbeitskreis Verteidigung des BITKOM auf die zentrale Rolle der ITK im Modernisierungsprozess der Bundeswehr hin.

Modernisierung darf sich nicht auf die verwaltungsinterne Domäne beschränken. ITK werden dann zu Effizienzsteigerungen führen, wenn ihr Potenzial im querschnittlichen Einsatz verstanden wird. Modernisierung ist zudem keine Einbahnstraße: Ohne die langjährige Expertise der deutschen Industrie und deren Einbringung in Forschung, Entwicklung und Bereitstellung der benötigten Spitzentechnologie vor Ort kann die Technologielücke zu unseren NATO-Partnern nicht geschlossen werden.

Industrielle Fähigkeiten nutzen heißt Bündnisfähigkeit stärken: Seit dem Ende des Kalten Krieges haben sich sicherheitspolitische Prioritäten verschoben. Damit einher ging die massive Reduzierung der wehrtechnischen Industrie – im Übrigen ein Prozess, von dem auch die deutsche ITK-Wirtschaft als eng verbundener Industriezweig nicht unbeeinflusst blieb. Umso wichtiger ist es, am Standort Deutschland vorhandene Fähigkeiten zu nutzen und sie dort einzusetzen, wo es am nötigsten ist: Beim Nutzer, nicht allein beim Planer.

Kooperation braucht Transparenz: Die im BITKOM versammelte deutsche ITK-Industrie vereint das technologische Wissen, das der „Kunde“ Bundeswehr für die iterative Anpassung seiner Fähigkeiten und materiellen Ausstattung benötigt. Ähnlich einem System verbundener Röhren nimmt die Bundeswehr automatisch am Innovationsprozess der primär im zivilen Sektor tätigen Industrie teil und kann mit geringem Adaptionsaufwand eigene Projekte zum Erfolg führen.

Im Anschluss an die vor zwei Jahren erschienene Publikation des BITKOM gibt die vorliegende Broschüre einen Überblick über Services und Lösungen, die den aktuellen technologischen Stand der Informations- und Kommunikationstechnologie darstellen bzw. im internationalen Kontext bereits eingesetzt werden. In kurzen Abschnitten werden diejenigen Technologien und Dienste beschrieben, die für den Nutzer Bundeswehr von besonderer Bedeutung sind. Einsatzbeispiele verdeutlichen die Relevanz der ITK-Wirtschaft und deren Mehrwert für die Bundeswehr. Das Bild wird durch technische Exkurse vervollständigt.

Jörg Menno Harms

2 Disruptive Technology – die Sprengkraft von Informations- und Kommunikationstechnologien

Angesichts der unbestrittenen Innovationskraft, die die Informations- und Kommunikationstechnologien auszeichnet, scheint die Frage nach wirklich Neuem, „Zerreißendem“ recht trivial. Dennoch: So wie die digitale Fotografie nach und nach die klassischen chemischen Filme vom Markt verdrängt hat, zeichnen sich auch in der Informations- und Kommunikationstechnologie Entwicklungen ab, die Anlass zu hohen Erwartungen geben.

War es in der Vergangenheit noch eine wichtige Aufgabe, ITK-Lösungen besonders schlank, also ressourcensparend zu realisieren, hat sich dieser Zwang heute praktisch erübrigt. Getrieben von den rasanten Entwicklungen im Massenmarkt stehen heute Übertragungsbandbreiten, Rechenleistung und Speicherkapazitäten in schier unbegrenzter Menge zu vergleichsweise sehr niedrigen Kosten zur Verfügung.

Informationen lassen sich heute nahezu beliebig speichern, sichern und verarbeiten. Der Zugriff auf Informationen geschieht zu jeder Zeit und von jedem Ort. Das erzeugt völlig neue Modelle und Prozesse der Informationsaufbereitung mit dem Ziel, dem eigentlich limitierenden Element, dem Menschen zu dienen.

Im zivilen Markt zwingen die schier unendliche Heterogenität und das Fehlen steuernder Autoritäten zur Interoperabilität auf Basis von (Quasi)-Standards. Mit Erfolg! Niemand diskutiert Datenmodelle und Übertragungswege. Was verfügbar ist, wird verwendet, was nicht, verödet. Mit jeder technischen Innovation ändert sich die ITK-Welt um uns herum in kleinen Schritten. Informations- und Kommunikationstechnologien werden damit zu ubiquitär verfügbaren Bestandteilen unserer Erfahrungswelt.

Es geht daher in dieser Broschüre um weit mehr als eine Betrachtung der ITK unter dem Aspekt der Produktivitätssteigerung und der Schaffung neuer Wertschöpfungsketten im öffentlichen Sektor. ITK sind der Hebel der Transformation. Im Prozess der Modernisierung sind sie eine unumgängliche Option, wirken im Zusammenspiel mit Entscheidungen auf politisch-administrativer Ebene und verändern somit in autoreflexiven Prozessen die Institutionen, in die sie selbst eingebettet sind.

Ein „Grand Dessein“ von ITK-Lösungen tritt angesichts dieser Entwicklungen in den Hintergrund, minimalinvasive Entwicklungsschritte versprechen mehr Aussicht auf Erfolg. Mit Entstehen der sogenannten Service Oriented Architectures (SOA) und der darin verwendeten standardisierten Module, Schnittstellen und Sprachen werden solche Ideen

Wirklichkeit. Bestehende Applikationen lassen sich sukzessive verbinden und in eine neue, integrierte Architektur migrieren.

Think big – start small, dieser Leitsatz ist das eigentlich Umstürzende, das Vorhandensein der dafür notwendigen Technologie ist dann tatsächlich – im positiven Sinne – trivial.

3 Aufbau der Matrix: Die Infostructure als Basis der Befähigung zur vernetzten Operationsführung

Bei der Realisierung der netzwerkbasierten Operationsführung (NetOpFü) gewinnt die Integration von Kommunikationsinfrastrukturen zunehmend an Bedeutung. In der NetOpFü-Konzeption sind Aufklärungs-, Führungs- und wirkungsorientierte Systeme nicht nur miteinander vernetzt, sondern partizipieren teilstreitkraftübergreifend am gemeinsamen Information Grid der Bundeswehr.

Diese Partizipation ist unabdingbare Voraussetzung für die Erstellung des gemeinsamen, ebenen- und auftragsgerechten Lagebilds. Weltweite Verfügbarkeit als zusätzliche Anforderung ergibt sich aus der angepassten Auftragsstruktur der Bundeswehr. Entsprechend den Anforderungen zur Unterstützung des weltweiten Einsatzes ist die Kommunikationsinfrastruktur, die seit Jahrzehnten innerhalb Deutschlands für die Bundeswehr bereitgestellt wird, zu erweitern.

Neue technologische Denkansätze vergrößern die Handlungsoptionen für NetOpFü. Das vorliegende Kapitel betrachtet die Infostructure, d. h. die Informations- und Kommunikationsinfrastrukturen sowie deren konzeptionelles und technologisches Umfeld.

3.1 Service Oriented Architecture: Ausgangspunkt für flexibles Handeln

Moderne Organisationen müssen in der Lage sein, schnell und flexibel auf neue Anforderungen und Situationen zu reagieren, Mobilität und auch Sicherheit zu gewährleisten. Bei steigender organisationsinterner und -externer Komplexität sind möglicherweise anfallende Kosten zu berücksichtigen; parallel führen Entwicklungen wie Outsourcing, Offshoring oder auch Unternehmenszusammenschlüsse zu anspruchsvolleren IT-Architekturen.

Effizienz, Agilität und Kosteneffizienz durch SOA

Im privatwirtschaftlichen und öffentlichen Bereich definieren sich demnach die Anforderungen an IT-Strukturen wie folgt: Sie sollen agiler werden, um schnell auf neue Bedürfnisse reagieren zu können und die Wiederverwendbarkeit von Komponenten besser als bisher zu erlauben sowie gleichzeitig offen sein, um die Abhängigkeit von einzelnen Herstellern zu vermeiden und Investitionen zu schützen.

Auch bei der Bundeswehr ist eine Vielzahl von Systemen mit umfangreichen Fähigkeiten im Einsatz. Im Zuge der Transformation hin zu vernetzter Operationsführung ist es notwendig, die Fähigkeiten einem erweiterten Nutzerkreis (in Joint und Combined

Operationen) zugänglich und nutzbar zu machen. Dies wird unterstützt durch die Komponentenbildung in den Systemen und die Schaffung der Möglichkeit zur Re-Komposition von einzelnen Diensten zu Verbundanwendungen auf Basis von Service Oriented Architecture (SOA).

Informations- und Kommunikationstechnologien – wo wir heute stehen

IT-Infrastrukturen sind meist über Jahrzehnte gewachsen. Das Hinzukommen neuer, innovativer Anwendungen und Systeme, der Druck der Kostenreduzierung und Wiederverwendung führt die IT-Abteilungen verschiedener Organisationen dazu, Systeme auch über Abteilungsgrenzen hinweg miteinander zu verbinden, um Anwendungen und Business-Komponenten gemeinsam nutzen zu können.

Zwar fanden neben Punkt-zu-Punkt-Verbindungen bereits modernere Technologien wie Message-Oriented-Models (MOM) oder Anwendungsintegrationssysteme (Enterprise Application Integration, EAI) Anwendung. Sie basierten jedoch meist auf proprietären Schnittstellen, Protokollen und Datenmodellen, was zu noch größerem Architekturchaos und Abhängigkeiten geführt hat. Durch fest verdrahtete Abhängigkeiten kann wiederum nur schwerfällig und langsam auf neue Anforderungen reagiert werden; übergreifende Informationsprozesse können durch starre IT-Architekturen kaum und nur aufwendig angepasst werden. Damit sind unmittelbar hohe Kosten und zeitlicher Aufwand verbunden. Darüber hinaus erschwert die Zuordnung einzelner IT-Assets zu bestimmten Anwendungen die organisationsübergreifende Verwendung. Ergebnis sind Duplikationen und damit unnötige Kosten. Eine Lösungsmöglichkeit wird durch die SOA geboten.

Strukturelemente der SOA

Allgemeingültige Elemente einer SOA lassen sich wie folgt festhalten: Es handelt sich zunächst nicht um eine Technologie oder ein Produkt, sondern um Prinzipien und Methoden für das Design von Anwendungen bzw. Architekturen auf Basis wieder verwendbarer, verteilter und gemeinsam genutzter Dienste. Als Dienst ist dabei eine businessorientierte Software-Komponente zu verstehen, die durch ihren Namen über Anwendungen und sogar Unternehmen hinweg aufgerufen werden kann und über eine dokumentierte, programmatische Schnittstelle verfügt.

Im Gegensatz zum klassischen EAI-Ansatz, bei dem es hauptsächlich darum geht, die vorhandenen monolithischen und isolierten Anwendungen zum Zwecke der Prozessautomatisierung und -optimierung miteinander zu verbinden, geht SOA einen Schritt weiter und zieht zusätzliche Abstraktionsebenen ein. In diesem Kontext entstehen schließlich wiederverwendbare und lose gekoppelte Dienste, die eine dedizierte Business-Funktionalität abbilden. Diese können flexibel zu so genannten Verbund-Anwendungen zusammengefügt und orchestriert werden. Damit macht eine SOA die Heterogenität einer historisch gewachsenen IT-Basis wesentlich kontrollierbarer und einfacher handhabbar.

Die wesentlichen Eigenschaften einer SOA lassen sich somit in drei grundlegenden Prinzipien zusammenfassen:

- Logische und physikalische Trennung der Geschäftslogik von der Präsentationslogik;
- Aufspaltung der Geschäftslogik bzw. -abläufe in unabhängige Einzelmodule bzw. Dienste;
- Kapselung der Funktionalität bzw. Implementierung der einzelnen Services über definierte Service-Schnittstellen.

SOA ist per se technologieneutral. Dennoch haben sich in den letzten Jahren einige wesentliche Technologien und Standards etabliert, die sich für die Implementierung einer SOA empfehlen. Insbesondere sind hier WebServices zu nennen, die folgende Aufgabenstellungen standardisieren:

- Dienste-Aufruf (Service Oriented Architecture Protocol, SOAP, ehemals Simple Object Access Protocol);
- Service-Beschreibung (WebServices Definition Language, WSDL);
- Zusammenführung einzelner Dienste zu Verbundanwendungen (WebServicesIntegration, WS-I);
- Definition von Prozessen, die regelbasiert und ereignisgesteuert die Inanspruchnahme von Services regeln (Business Process Execution Language,WS-BPEL).

Im Rahmen der Evolution offener Plattformen und Laufzeitumgebungen finden sich die Implementierungen dieser Standards einerseits in der Eclipse-Anwendungsentwicklungs-Umgebung und andererseits in den Laufzeitumgebungen der führenden Applikations-Server wieder.

Vorteile nutzen – Vorsprung realisieren

Organisationen werden durch SOA in die Lage versetzt, einfacher und schneller auf neue Situationen und Herausforderungen reagieren zu können: Einerseits durch die schnellere Verfügbarkeit von relevanten und akkuraten Informationen, auf deren Basis Entscheidungen getroffen werden, andererseits durch schnellere und effizientere Anpassung bzw. Erstellung neuer Informationsprozesse. Der höhere Anteil wiederverwendbarer Services und vorhandener IT-Assets sowie die flexibleren und besser anpassbaren Infrastrukturen erzielen erhebliche Kosteneinsparungen in neuen IT-Projekten und bei der Pflege vorhandener IT-Infrastruktur. Die Unabhängigkeit von der eingesetzten Technologie schafft Unabhängigkeit von speziellen Herstellern und damit mehr Freiräume bei der Wahl von Produkten.

Mit SOA zu einer iterativen, ergebnisorientierten Herangehensweise

Eine SOA-Infrastruktur erlaubt einen schrittweisen Ansatz für neue Projekte und Services und korrigiert damit das Ungleichgewicht zwischen den stetig sich ändernden Geschäftsanforderungen und den Einschränkungen einer bislang starren Infrastruktur. Mit SOA lässt sich die Erfolgsquote für IT-Projekte steigern.

Die Serviceorientierung erlaubt bessere und klarere Planung und Dokumentation, erleichtert die Integration von bestehender und neuer Funktionalität und erlaubt den einfacheren Einbezug der Fachabteilungen. Sie minimiert das Risiko, dass Erwartungen der Fachabteilungen nicht erfüllt werden.

SOA erlaubt ferner die Einführung von neuer Funktionalität in kleinen Schritten, Probleme können frühzeitig erkannt und korrigiert werden. Somit zeigt sich, dass SOA neben der höheren Agilität eine Reihe weiterer Vorteile für die Organisation bedeuten kann.

3.2 Das Netz – Nervensystem der Bundeswehr

Mit der Konnektivität wird die Verfügbarkeit aller Daten und der Zugriff darauf von überall und zu jeder Zeit gewährleistet. Dabei ist Internet Protocol (IP) der zivile Standard, aber auch der Anschluss von proprietären Kommunikationssystemen muss transparent möglich sein.

Informations- und Kommunikationstechnologien – wo wir heute stehen

Zivile High-Tech als Ausgangspunkt für den militärischen Bereich

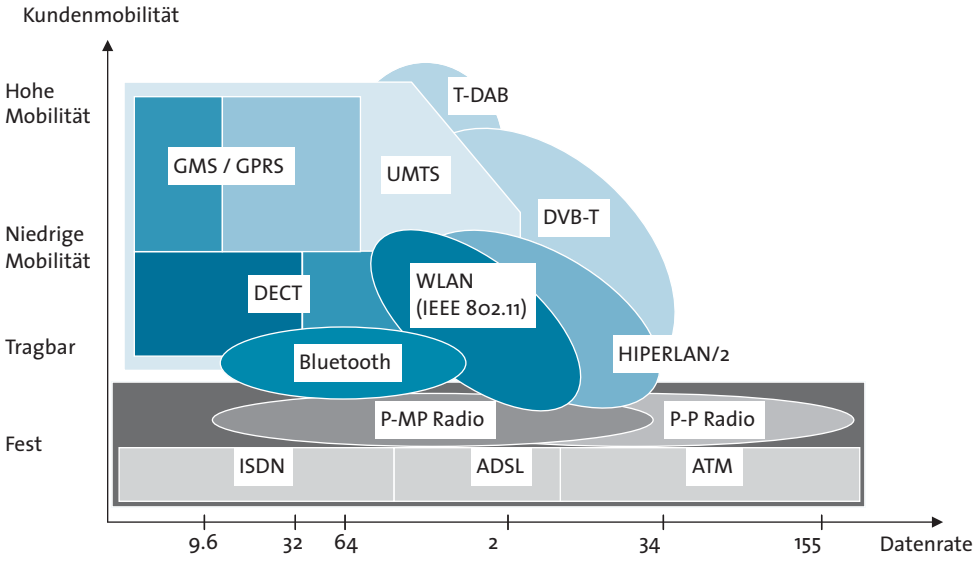
Den aktuellen Stand der Technologie stellt heute IP-basierte Infrastruktur dar. Diese bildet Sprache und Daten auf einem einzigen Netz ab. Eine solche Infrastruktur ist durch die angewandte MPLS-Technologie diensteunabhängig und stellt durch die standardmäßig bereitgestellte „Any-to-any Connectivity“ bereits auf der untersten Netzebene die geforderte Flexibilität eines zukunftsorientierten Wide Virtual Network (WVN) zur Verfügung.

Dies bedeutet unter anderem minimalen Administrationsaufwand und einfache Bedienung durch intelligente Netz- und Endgerätefunktionen. Mit MPLS wird die Übertragungsgeschwindigkeit erhöht und die Bildung von beliebig vielen VPN möglich. Weiterhin werden wichtige Leistungsmerkmale wie Priorisierung (Quality of Service, Class of Service) und die Möglichkeit zur digitalen Sprachübermittlung (Voice over IP, VoIP) genutzt. Plattformorientierte Technologien ermöglichen flexible Bandbreitennutzung und die Bereitstellung der benötigten Redundanzen. Durch die Festschreibung von Service Level Agreements und den Einsatz von aktivem Netzmanagement werden schon heute Verfügbarkeiten von nahezu 100% erreicht.

Die Verknüpfung mit mobilen Netzen und Satellitenübertragungskapazitäten bietet eine Kommunikation mit allen verfügbaren Diensten an nahezu jedem Ort der Welt. Mobile Übertragungstechniken wie TETRA, GSM, UMTS, WLAN und WiMAX werden zunehmend im Bereich verlegefähige Adhoc-Netze benötigt.

Um den hohen Anforderungen an die IT-Sicherheit gerecht zu werden, werden zusätzlich zu der sicheren, von anderen Kunden getrennten Datenübertragung im IP-Netz alle Daten (Sprache und Daten) über Internet Protocol Security (IPSec) verschlüsselt. Zusätzliche

Sicherheit bieten angewandte Verfahren (zum Beispiel ALLA/NALLA), die eine Abbildung der Leitungsdaten in elektronischen Systemen „unsichtbar“ machen.



CSM	Global System for Mobile Communication	HIPERLAN	High performace Radio LAN
GPRS	General Packet Radio Service	T-DAB	Terrestrial Digital Audio Broadcasting
UMTS	Universal Mobile Telecommunications System	DVB-T	Digital Video Broadcasting Terrestrial
DECT	Digital Enhanced Cordless Telecommunication	P-MP	Point-to-Multipoint
WLAN	Wireless Local Area Network	P-P	Point-to-Point

Abbildung 1: Übersicht moderner drahtloser Technologien

Wohin geht der Weg?

In naher Zukunft wird die Übertragung von Daten über so genannte Next-Generation-Networks (NGN) realisiert. Die dann klassischen VPN (ATM, DSL, PSTN, IP etc.) werden unter einem NGN zusammengefasst und gemanagt. Dadurch wird die gleichzeitige Übermittlung von Sprache, Daten und Video (Triple Play) möglich.

Triple Play – zu Hause und im Einsatz

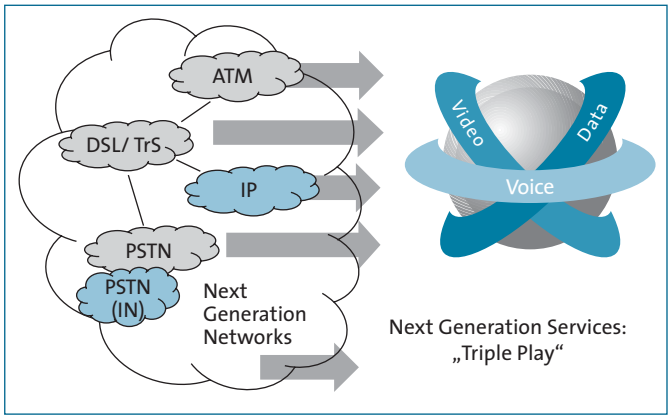


Abbildung 2: Next Generation Networks

Vorteile nutzen – Vorsprung realisieren

Durch die militärische Mitnutzung zivil vorhandener Netze stellt sich mehr und mehr die Frage nach dem Bedarf eigener dedizierter Netze. Viele Leistungsmerkmale und Technologien, die im Massenmarkt etabliert sind, genügen auch den Anforderungen militärischer Nutzung. Vorteile ergeben sich – und das gilt für nahezu alle aufgeführten Technologien und Dienste – aus dem automatischen Nutzen der Innovationszyklen und ständig aktueller Erweiterungen des Leistungsspektrums. Wirtschaftlich steht dem Nutzer der gesamte ITK-Markt zur Verfügung. Darüber hinaus werden eigene Entwicklungs-, Betriebs- und Servicekosten eingespart.

Dedizierte Netze oder Aufbau auf Vorhandenem?

Mit geringem Adaptionsaufwand zum Erfolg

Durch die Einführung der IP-Technologie und den Einsatz offener Systeme wird sich generell der Aufwand zur Adaption auf militärische Anwendungen verringern. Für die Nutzung sog. schwarzer Netze ist im Großteil der Fälle kein weiterer technologischer Aufwand nötig.

Sog. rote Netze können durch den Einsatz von End-to-End-Verschlüsselung abgebildet werden. Unterstützend können zusätzlich Tunnel- und Krypto-Mechanismen sowie die Bildung von VPN genutzt werden.

Einsatzbeispiele

- Ein national flächendeckendes Netz für Datenübertragung.
- Ein national flächendeckendes Netz für Sprachübertragung.
- Verlegefähige IP-Netze (Adhoc-Netze) für Einsatzgebiete.
- Mobilfunknetze (GSM, UMTS, GPRS, TETRA).
- Sichere Einwahllösungen inkl. mobiler Komponenten (IP-Secure VPN).

3.3 Access

Mit der Access-Schicht wird die Berechtigung des sicheren, geschützten Zugriffs ebenso wie die Authentizität und Unverfälschbarkeit der Daten sichergestellt.

3.3.1 Sicherer Zugang zum Netz: PKI

Informations- und Kommunikationstechnologien – wo wir heute stehen

Sicherer Zugang zum Netz mit PKI

Public Key Infrastructure (PKI) beschreiben Regeln zur Erzeugung, Ausgabe und Anwendung von Zertifikaten als elektronischer Identitätsnachweis auf Basis hochwertiger Schlüsselmittel (zum Beispiel Smartcards) und kryptographischer Verfahren. Auf der Basis einer PKI erfolgt in IT-Anwendungen und Systemen die Sicherung von Daten bzw. Informationen im Hinblick auf Authentizität, Integrität und Vertraulichkeit.

Stand der Technik ist heute die Chipkarte mit Kryptoprozessor, eine Schlüsselerzeugung in der Hochsicherheitsumgebung eines zertifizierten Trust-Centers, die sichere Speicherung der Schlüssel und die Durchführung aller Operationen mit dem geheimen Schlüssel in der Karte.

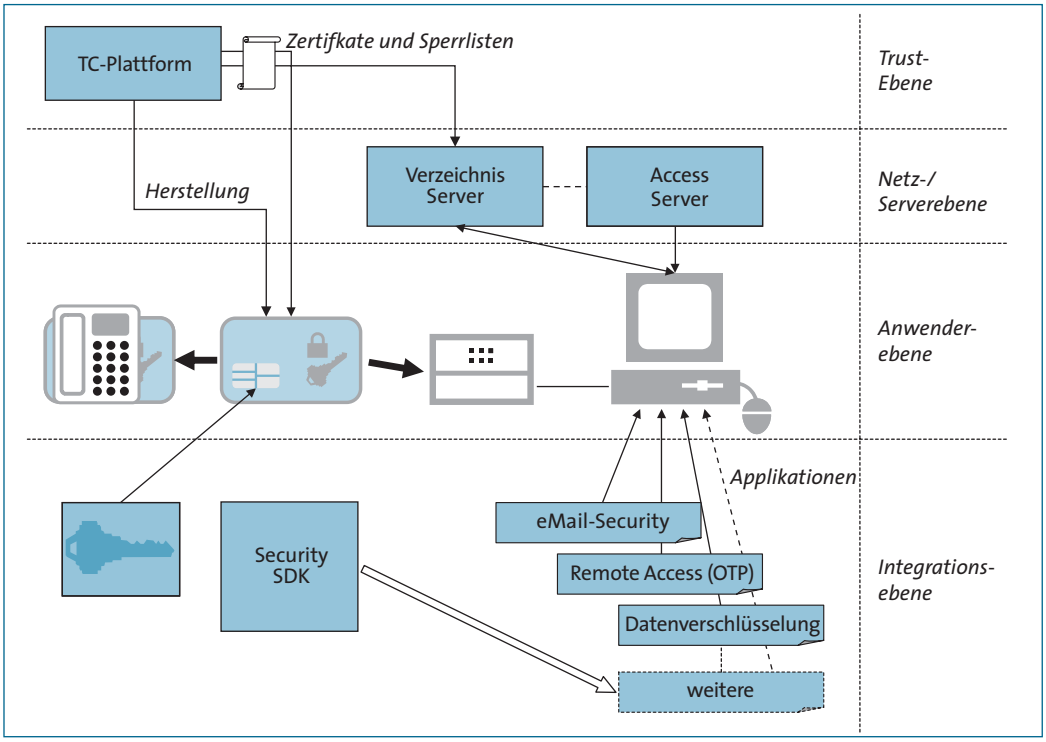


Abbildung 3: Public Key Infrastructure

Die vom Trustcenter vergebenen Zertifikate enthalten Informationen zu der Zuordnung von Identifikationsdaten einer Person zu einem öffentlichen Schlüssel. Dabei werden im Regelfall der Name, die Adresse, die Firmenzugehörigkeit und die E-Mail-Adresse gespeichert und durch eine digitale Signatur des Trust-Centers beglaubigt.

Mit der Nutzung einer PKI wird die Authentizität der Daten sichergestellt, der Absender kann eindeutig identifiziert werden und die Dateien sind vor Manipulation während der Übertragung geschützt. Zudem erfolgt der Zugriff auf Anwendungen und Daten rollen- und aufgabenbasiert, das heißt, dass nur autorisierte und identifizierte Nutzer zugreifen können.

Vorteile nutzen – Vorsprung realisieren
Die benötigten Module zur Verwaltung der PKI-Ebenen sind:

- End Entity (EE) - Personen als Zertifikatsinhaber und Server als „Zertifikatsinhaber";
- Registration Authority (RA) – Identifizierung der User, Registrierung der User;
- Certification Authority (CA) – Ausstellung von Zertifikaten, Sperren von Zertifikaten, Bereitstellung von Zertifikatsinformationen;
- Public Key Directory (PKD) – Elektronisches Verzeichnis zur Veröffentlichung von Zertifikatsinformationen, – Zugang für Anwendungen und Systeme.

Diese stehen in der zivilen IT-Industrie vollständig zur Verfügung. Die Zertifizierung und Überwachung der Trust Center und IT-Security Dienstleister durch das Bundesamt für Sicherheit in der Informationstechnik ist gängige Praxis. Die Weiterentwicklung der Systeme erfolgt auf Basis von Standards, wie TLS/SSL, RSA, DES, SHA1, CMP*, LDAP, OCSP*, S/MIME, X.509.v3, RFC 2078, RFC 2459 (PKIX), PKCS#1, #3, #7, #9, #10, #11 und #12, IPSec, TLS/SSL, X.500, X.509, S/MIME. Somit ist auch die Interoperabilität gewährleistet.

Mit geringem Adaptionsaufwand zum Erfolg

Überschaubarer Adaptionsaufwand

Da die PKI auf allgemein gültige Standards aufsetzt, beschränkt sich der Adaptionsaufwand bei dem Einsatz im militärischen Umfeld auf die Gestaltung der Prozesse und die Abbildung der Organisation und Rollenkonzepte. Im administrativen Umfeld kann die zivile Hardware uneingeschränkt genutzt werden.

Anforderungen an militärische Härtung der HW bestehen nur im operativen Umfeld, z. B. Zugriffssteuerung auf Waffeneinsatzsysteme. Es können entweder die existierenden zivilen Trust-Center-Kapazitäten genutzt werden – Modell des Application Service Providing (ASP) – oder eigene Infrastrukturen mit Hilfe des vorhandenen zivilen Know-Hows aufgebaut werden – Commercial off the Shelf.

Einsatzbeispiele
Die Nutzung einer PKI gestattet rollen- und aufgabenorientierten Zugriff auf Informationen aus Führungsinformationssystemen sowie aus administrativen Systemen. Auch der Zugriff auf Waffensysteme kann somit rollen- und aufgabenbasiert reglementiert werden.
Daneben können allgemeine Funktionen, wie Zutrittskontrollen, Arbeitszeitkontoführung etc. abgebildet werden.

3.3.2 Sicherer Zugang zum Netz: Identity- & Access Management

Informations- und Kommunikationstechnologien – wo wir heute stehen

IAM als Bestandteil der IT-Sicherheit

Identity- und Access Management (IAM) ist ein noch relativ junger und dynamisch wachsender Markt, der in den vergangenen Monaten stark an Beachtung gewonnen hat und zunehmend als ein essentieller Teil der IT-Infrastrukturen auch von privatwirtschaftlichen Unternehmen betrachtet wird. Die Einführung von neuen, integrativen Identity-Management-Lösungen in Unternehmen wird in der Regel von einer Vielzahl von Faktoren getrieben.

So steht zum Beispiel in vielen Fällen das Thema IT-Sicherheit im Vordergrund, d. h. Vermeidung von Kosten und Nachteilen durch Nichteinhaltung von Sicherheitsanforderungen, also beispielsweise durch unberechtigte Zugriffe auf Daten durch frühere, in Systemen nicht gelöschte Mitarbeiter. Doch Sicherheit ist nur ein – wenn auch sehr wichtiger – Aspekt.

Ein weiterer Faktor lässt sich am besten mit „Ease of Use“ beschreiben, d. h. der Wunsch der Anwender nach Vereinfachung durch weniger Benutzer-IDs, weniger Kennwörter und Self Service für personenbezogene Daten oder nach mehr Prozessgeschwindigkeit und -qualität, aber auch der Wunsch von IT-Verantwortlichen und Administratoren nach Vereinfachung und verringerten Ausfallzeiten.

Vorteile nutzen – Vorsprung realisieren

Kernbereiche des IAM

Das Angebot der deutschen ITK-Wirtschaft im Identity- und Access- Management umfasst heute acht Kernbereiche. Alle Lösungselemente sind auch autark nutzbar. Damit kann die Bundeswehr ihre Identity-Management-Infrastruktur Schritt für Schritt entwickeln und bestehende Lösungen, wie zum Beispiel die PKI-Infrastruktur oder SINA-Technologien integrieren.

Directories

1. Directories spielen in jeder IAM-Strategie eine zentrale Rolle. LDAP-Verzeichnisse vermitteln die Kommunikation zwischen dem Client (beispielsweise einem Mail-Server, einem Authentifizierungsdienst oder einem Adressverzeichnis) mit dem Directory-Server, um auf die gespeicherten Identitätsinformationen zugreifen und diese modifizieren zu können. Allerdings werden heute bei der Bundeswehr einerseits viele LDAP-basierende Verzeichnisdienste eingesetzt, andererseits aber auch noch proprietäre

Lösungen ohne LDAP-Unterstützung. In der Praxis führt dieses Nebeneinander zu Doppel- und Dreifachaufwand, Mehrkosten und häufigen Fehlern bei Eingabe und Verwaltung der Benutzerdaten. Die deutsche ITK-Wirtschaft kann der Bundeswehr leistungsfähige Verzeichnisdienste und gleichzeitig die Integrationslösungen für die Verbindung mit bestehenden Verzeichnisdiensten liefern. Damit hat die Bundeswehr die nötige Offenheit bei ihrer Verzeichnisdienststrategie, gleichzeitig aber die Lösungsansätze, um die Datenqualität über verschiedene Verzeichnisse hinweg zu verbessern und den administrativen Aufwand zu verringern.

2. Virtual Directories versprechen hier rasche Abhilfe; dies gilt gerade in der komplexen Anwendungslandschaft der Bundeswehr, in der mehrere Verzeichnissysteme parallel betrieben werden. Das Virtual Directory verbindet Identitätsdaten aus Verzeichnisdiensten, Datenbanken und Textdateien in Echtzeit miteinander, um zuverlässige Zugangskontrolle für Applikationen, Verfahren und Prozesse zu ermöglichen. Außerdem lassen sich Verzeichnisdaten für administrative und andere Anwendungen in fast beliebiger Weise strukturieren.

Virtual Directories

3. Access & Identity sind Bereiche, mit denen sich die ITK-Branche schon seit längerem beschäftigt. In komplexen vernetzten Umgebungen wird aber das Thema einer Vereinfachung beim Anmelde- und Rechtemanagement aus Benutzersicht immer kritischer. Durch Single-Sign-on Lösungen und Delegated Administration Services stehen der Bundeswehr heute ausgereifte und vollständige Lösungsansätze zur Verfügung, die sich flexibel, skalierbar und sicher an unterschiedliche Bedürfnisse der Bundeswehr anpassen lassen und zudem die Kosten für die Einhaltung regulatorischer Vorschriften („Compliance“) deutlich senken.

Access & Identity

4. Provisioning (Bereitstellung) ist ebenfalls ein Teil des Identitäts-Managements, bei dem erforderliche Ressourcen (IT-Systeme) für die Anwender automatisch bereitgestellt werden. Da es heute immer häufiger in Unternehmen um digitale Zugangsberechtigungen geht, spricht man in diesem Zusammenhang häufig auch von „eProvisioning“. Die deutsche ITK-Wirtschaft bietet besonders anpassungsfähige Lösungen und zwingt die Bundeswehr nicht dazu, in teuren Anpassungsaufwand zu investieren, um lückenlos in bestehende Geschäftsprozesse und Arbeitsabläufe integriert zu werden.

Provisioning

5. Federation eröffnet der Bundeswehr die Möglichkeit, ihren externen Partnern sicheren Zugriff auf Informationen zu gewähren, auch wenn diese auf unterschiedlichen Systemen über die Bundeswehrgrenzen hinweg gespeichert sind. Dazu werden weltweit standardisierte Federation-Protokolle genutzt, um mehrere Nutzerkonten mit unterschiedlichen Online-Anbietern zu verbinden. Dies sorgt für eine sichere Authentifizierung und bietet dem User den Vorteil, dass er sich nur einmal anmelden muss. Navigiert ein Nutzer auf unterschiedlichen Websites, die zur selben Federation gehören, erkennt die Software seine Identität und kann auf Basis seiner persönlichen Präferenzen eine sichere Umgebung bereitstellen.

Federation

Digitale Zertifikate

6. Digitale Zertifikate, auch digitale IDs genannt, sind die elektronischen Gegenstücke zu Dienstausweisen, Firmenausweisen, Führerscheinen oder Reisepässen. Ein digitales Zertifikat kann auf elektronischem Wege zum Nachweis der Identität des Benutzers oder seiner Zugriffsrechte auf Informationen oder Online-Dienste vorgelegt werden. Eine entprechende PKI-Strategie der Bundeswehr kann somit zu jeder Zeit in eine Gesamtsicherheitslösung integriert werden. Die Produkte sind leicht zu implementieren und bieten das Ausstellen und Verwalten von digitalen Zertifikaten durch den Benutzer selbst über ein entsprechendes Web-Interface.

Web Services

7. Web Services sind Software-Bausteine, die mit Anwendungen über das Internet oder Intranet kommunizieren können. Mit ihrer Hilfe kann die Bundeswehr Web Services interner und externer Anbieter und Partner zu komplexen neuen Anwendungen kombinieren.

Security Tools

8. Security Tools sind kritische Elemente und Werkzeuge bei der Applikationsentwicklung. Immer häufiger schreiben bundeswehrinterne oder regulatorische Richtlinien den Schutz von vertraulichen bzw. persönlichen Daten zwingend vor. Der Aufwand für die Eigenentwicklung solcher Systeme wäre enorm. Marktgängige Werkzeuge senken die Kosten und den Zeitaufwand für die Bundeswehr, indem sie einen Baukasten von kryptographischen Elementen zur Verfügung stellen, mit deren Hilfe sich selbst komplexe SOA-Projekte vergleichsweise schnell und einfach realisieren lassen.

Dabei werden Identitätsdienste nicht nur für Administratoren, sondern auch für Anwendungsentwickler bereitgestellt. Durch die Nutzung einer zentralen Identity-Management-Infrastruktur lassen sich neue „Identitätsinseln“ und daraus resultierende hohe administrative Kosten vermeiden.

3.3.3 Sicherheit im Netz: Absicherung von Netzwerkübergängen

Firewalls gewinnen seit etwa fünfzehn Jahren an Bedeutung, um Bereiche von IT-Netzen vor Gefährdungen aus anderen, verbundenen Netzen zu schützen.

Informations- und Kommunikationstechnologien – wo wir heute stehen
Der Hauptzweck einer Firewall besteht in der Kontrolle des Datenaustausches zwischen IT-Netzen mit unterschiedlichen Sicherheitsniveaus. Firewalls bieten je nach eingesetztem Typ unterschiedliche Schutzfunktionen von der Einschränkung unbenötigter Kommunikationswege bis zur Inhaltskontrolle der übertragenen Daten.

Firewall-Typen

Es existieren verschiedene Typen von Firewall-Systemen, die sich vom grundsätzlichen Ansatz und damit auch in der Implementierung sehr voneinander unterscheiden. Aufgrund ihrer spezifischen Arbeitsweise können diese Firewall-Typen unterschiedliche Schutzfunktionen realisieren.

1. Paketfilter-Firewalls arbeiten auf der Netzwerk- und Transportschicht-Ebene des ISO/OSI-Netzwerkmodells. Sie können Pakete aufgrund von IP-Adresse, Protokolltyp, Port-Nummer und gegebenenfalls TCP/IP-Flags filtern. Statische Regeln legenfür eine Kombination dieser Kenngrößen fest, ob ein IP-Paket weitergeleitet wird oder nicht. Paketfilter-Firewalls dienen in erster Linie der Festlegung akzeptierter Kommunikationswege, eine inhaltliche Kontrolle der übertragenen Daten ist damit nicht möglich.

Paketfilter

2. Stateful Paketfilter-Firewalls führen zusätzlich Tabellen über den Status von Verbindungen und erlauben damit eine intelligentere Filterung von Paketen als normale Paketfilter. Abhängig vom Verbindungsstatus können sie dynamisch weitere Kommunikationswege öffnen, um beispielsweise Antwortpakete zu akzeptieren. Sie bieten damit zusätzliche Sicherheit, da viele Ports für von außen kommende IP-Pakete nicht permanent offen sein müssen. Eine Inhaltskontrolle ist aber auch mit diesem Firewall-Typ nicht möglich.

Stateful Paketfilter

3. Applicationlevel Gateways (auch Proxy-Firewalls genannt) überprüfen die übertragenen Daten zusätzlich inhaltlich auf den ISO/OSI-Ebenen 4 bis 7 (Transport- bis Anwendungsschicht). Diese Schutzart wird mittlerweile immer wichtiger, weil Angreifer grundsätzlich akzeptierte und benötigte Protokolle wie WWW-Zugriff und E-Mail-Austausch für ihre Zwecke missbrauchen. Solch ein Missbrauch lässt sich nur durch die Analyse des Dateninhaltes erkennen und verhindern. Applicationlevel Gateways erkennen und blockieren deshalb Protokoll-verletzungen und Schadinhalte wie Viren, Würmer, Trojaner u. ä. Konfigurationsgesteuert filtern sie Daten anhand von Protokollelementen (z. B. kein FTP PUT), MIME-Types, Dateiart, Uniform Resource Locator (URL) und aktiven Inhalten (wie Java, JavaScript, ActiveX). Häufig werden auch effektive Maßnahmen zur Spam-Abwehr integriert. Applicationlevel Gateways integrieren daher eine hohe Zahl von Schutzfunktionen auf einer zentralen Plattform.

Applicationlevel Gateways

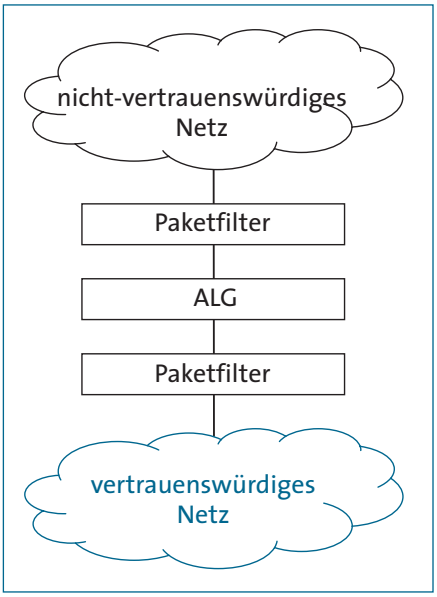


Abbildung 4:
Ein- bis dreistufiges Firewall-System

Es ist grundsätzlich ratsam, an Übergängen zwischen Netzen mit deutlich unterschiedlichen Gefährdungspotenzialen nicht einem einzelnen Firewall-System zu vertrauen, sondern stets mindestens zwei Firewall-Systeme hintereinander zu schalten. Dieser Grad an Absicherung wird beispielsweise an Übergängen zu Netzen mit hohem Schutzbedarf (mit Daten wie z. B. Personalbeurteilungen oder medizinischen Ergebnissen) benötigt.

Mehrstufigkeit: Hohe Sicherheit bei kritischen Informationen

Die Mehrstufigkeit eines Firewall-Systems bietet auch dann noch einen Schutz, wenn die externe Firewall von einem Angreifer übernommen und effektiv ausgeschaltet wird. Die zweite Firewall verhindert dann als weitere Verteidigungslinie, dass das interne Netz offen gelegt wird. Wichtig ist, dass die zweite Firewall nicht eine identische Kopie des ersten Systems ist, sondern dass sich die verwendete Firewall-Technik von der ersten unterscheidet. So können nicht beide Firewall-Systeme durch denselben Angriff ausgeschaltet werden.

Als besonders sicher gilt eine dreistufige Firewall in der Kombination Paketfilter – Applicationlevel Gateway – Paketfilter (PAP-Modell). Durch die symmetrische Anordnung wird das Herz des Firewall-Systems, das Applicationlevel Gateway, von beiden Seiten durch je einen Paketfilter geschützt. Gestärkt werden kann diese Anordnung durch Verwendung unterschiedlicher Paketfilter-Varianten. Diese Lösung wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlen.

Zertifizierung: Mehr Transparenz für den Nutzer

Durch das vielseitige und umfangreiche Angebot ist die technische Funktionsweise der einzelnen Firewall-Systeme für den Anwender sehr schwer durchschaubar. Eine Firewall ist ein sicherheitskritischer und wichtiger Bestandteil eines Netzes, auf deren fehlerfreie Funktion sich der Benutzer verlassen muss. Im Rahmen einer Zertifizierung nach Common Criteria oder ITSEC prüft und bewertet eine staatliche Zertifizierungsstelle die Funktionsweise und Sicherheitseigenschaften eines Firewall-Produktes und erteilt bei ausreichender Güte ein entsprechendes Zertifikat. Zertifikate nach Common Criteria EAL4 bzw. ITSEC E3 (oder höher) schließen dabei die Prüfung auf Quelltextebene mit ein.

Mit geringem Adaptionsaufwand zum Erfolg

Weitere qualitative Alleinstellungsmerkmale von Firewalls umfassen:

- Hochverfügbarkeit: Das Firewall-System sollte zu einer hochverfügbaren Lösung ausgebaut werden können.
- Skalierbarkeit: Durch die Bildung eines Clusters sollte der Datendurchsatz beliebig erweitert werden können.
- Wartbarkeit: Die Software muss einfach auf dem aktuellen Stand gehalten werden können. Außerdem sollte es möglich sein, die korrekte Funktion des Systems mit einfachen, integrierten Methoden zu überwachen und zu protokollieren.
- Anpassbarkeit: Das System muss flexibel an geänderte Anforderungen angepasst werden können.
- Selbstschutzfunktionen: Das Firewall-System muss sich selbst gegen unbefugte Änderungen schützen.

Einsatzbeispiele:

- Server-Firewall. Ein interner Server soll in der Regel nur einige wenige Dienste anbieten, deren Verfügbarkeit aber von großer Bedeutung ist. Der Zugang auf den Server sollte deshalb auf diejenigen Protokollports, die für diese Dienste notwendig sind, und auf den relevanten Clientenkreis beschränkt werden. Diese Zugriffsbeschränkung lässt sich

durch den Einsatz eines Stateful Paketfilters realisieren.

- Zonenbildung. Viele Netzwerke sind zwar über eine komplexe Firewall an das Internet oder an Netze mit niedrigerem Sicherheitsniveau angebunden, das interne LAN besteht aber aus einer flachen hierarchischen Struktur, die keine weiteren Sicherheitsübergänge enthält. Somit haben die internen Benutzer oft viele Zugriffsrechte, die dem Grunde nach nicht benötigt werden. Daher breiten sich eingeschleuste Viren und Würmer sehr leicht auf das gesamte Netz aus. Um die Sicherheit auch im internen Netz deutlich zu erhöhen, sollte es in logisch getrennte Segmente unterteilt werden, an deren Übergängen Stateful Paketfilter-Firewalls den Datenfluss kontrollieren.
- Anbindung von Liegenschaften. Diese Anbindung kann ebenfalls mit einem Stateful Paketfilter realisiert werden.
- Zonen/Systeme mit hohem Schutzbedarf. In Bereichen mit hohen Sicherheitsanforderungen, wie beispielsweise mit personenbezogenen Daten im Sanitäts- und Personalbereich, ist der Einsatz einer mehrstufigen Firewall mit Applicationlevel Gateway nahezu unumgänglich.
- Bereiche mit stark unterschiedlichen Sicherheitsniveaus. Dazu zählen beispielsweise Übergänge zum Internet, zu Lieferantennetzen oder auch vom WAN zu extrem sensiblen Bereichen. Solche Stellen laufen Gefahr, häufig und intensiv angegriffen zu werden. Um die Sicherheit im internen Netz zu garantieren, muss hier eine mehrstufige Firewall eingesetzt werden, am besten in P-A-P-Struktur.
- Rot-Schwarz-Übergänge. Die Absicherung dieser Übergänge kann nur durch hochwertige Spezialsysteme realisiert werden. Dabei müssen exzellente Methoden sicherstellen, dass keine Daten vom roten in das schwarze Netz gelangen und dass vom schwarzen Netz das rote Netz nicht angegriffen werden kann.

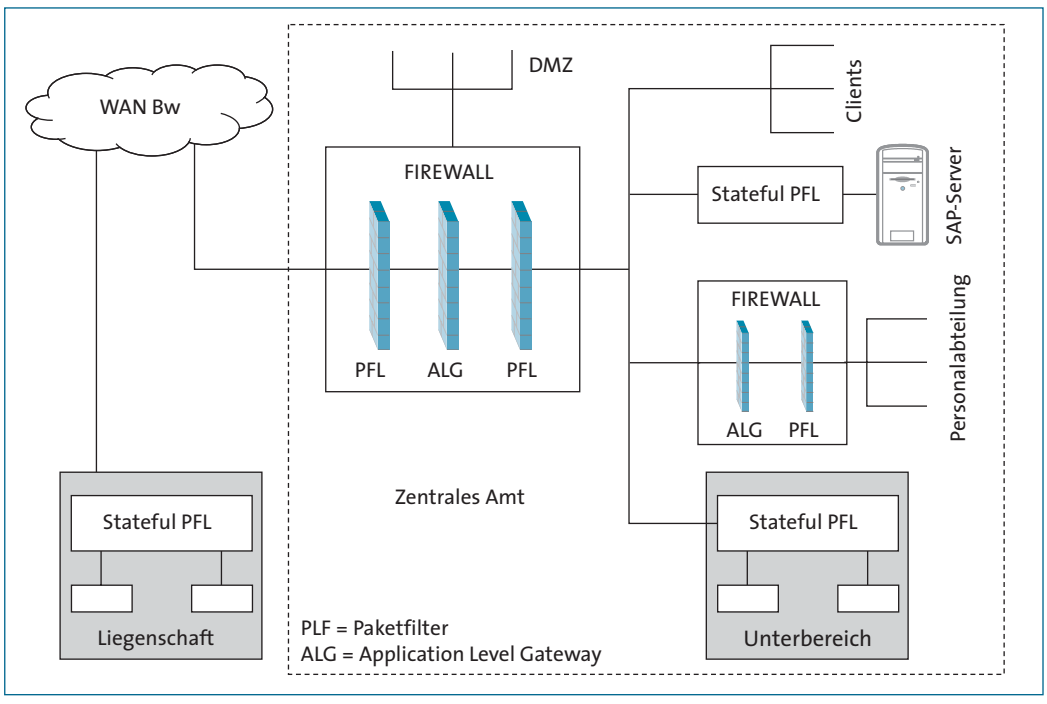


Abbildung 5: Beispielszenario (Zonenbildung, Bereiche mit unterschiedlichen Sicherheitsniveaus, Zonen mit hohem Schutzbedarf, Server-Firewall)

3.4 Hosting

Flexible Betreibermodelle: Make or buy?

Bei der Erörterung flexibler IT-Betreibermodelle stellt sich immer als erstes die Frage: „Make or buy“ – in eigener Verantwortung betreiben oder an einen Externen übergeben? Ist die Informationstechnologie noch Kerngeschäft? Als Ganzes oder in Teilen? Beim Hosting handelt es sich um ein Sourcing-Konzept, das neben der Outsourcing- Variante prinzipiell auch eine Inhouse-Option – insbesondere bei sensiblen Daten – offen hält. Damit kann und muss das IT-Betreibermodell auf die individuellen Anforderungen eines Kunden zugeschnitten werden.

Informations- und Kommunikationstechnologien – wo wir heute stehen
Im Gegensatz zu Outsourcing-Projekten, die in der Regel eine ganzheitliche Übernahm eines Teils der IT (samt Mitarbeitern) durch einen externen Dienstleister umfassen, wird bei Hosting die Dienstleistung durch einen externen Partner erbracht. Nachfolgende Unterscheidungsmerkmale sind bei der Ausgestaltung der Betreibermodelle relevant:

1. Housing: Verbleibt die IT-Infrastruktur in den eigenen Räumlichkeiten, wird von Inhouse-Hosting gesprochen (Betrieb im eigenen Rechenzentrum). Bei einem Betrieb außerhalb der eigenen Räumlichkeiten ist noch die reine Housing- Variante erwähnenswert. Hierbei wird nur die Gebäudeinfrastruktur (Raum, Strom, Kühlung, ...) zur Verfügung gestellt. Diese Variante wird hier nicht weiter verfolgt.

2. Nutzung der Infrastruktur: Unterschieden wird nach der Art der Kapazitätsbereitstellung, d. h. fester Zuordnung versus Flexibilisierung der Kapazitätsanpassungen (Utility-Ansatz). Darüber hinaus lässt sich die Nutzung der Infrastruktur nach Kundenzuordnung differenzieren. Möglich sind das Hosting für einen Kunden oder gemeinsame Nutzung durch mehrere Kunden, das sog. Shared Hosting.

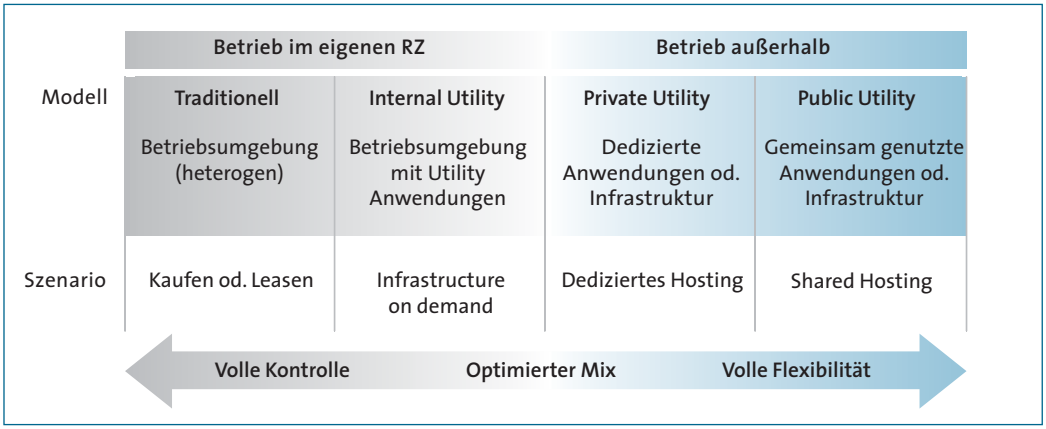


Abbildung 6: Unterschiedliche Betriebsmodelle bei Hosting

3. Geltungsbereich des Hosting-Ansatzes: Möglich sind Infrastruktur-Hosting, d. h. Bereitstellung und Betrieb von Rechner-, Speicher-, Netzkapazitäten, als auch

Anwendungs-Hosting. Letzteres kann SAP-Hosting, Hosting von Officeanwendungen, Web-Hosting und Hosting weiterer Anwendungen beinhalten.

4. Preismodell des Hosting Vertrages: In Zusammenhang mit der Flexibilisierung der Kapazitäten ist auch eine Variabilisierung der Preismodelle wahrnehmbar. Die oft damit einhergehende Entscheidung, die IT-Assets aus der kundeneigenen Bilanz zu nehmen und auf den Dienstleister zu übertragen, erleichtert diese Variabilisierung.

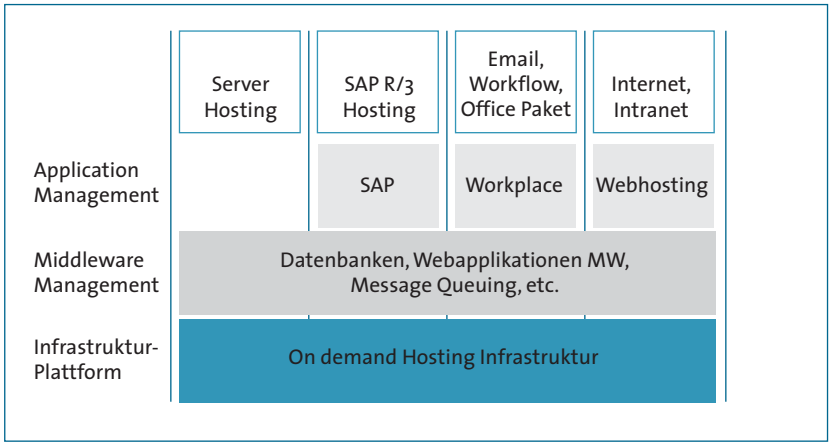


Abbildung 7: Welche Services werden vom Hosting-Provider geleistet?

Mit geringem Adaptionsaufwand zum Erfolg

Hosting. On Demand!

Der Trend beim Hosting geht eindeutig in Richtung bedarfsabhängige IT-Versorgung. Wesentliche Eckpfeiler dieses On-Demand-Prinzips sind variable und vielfach innovative Preis- und Finanzierungsmodelle, verknüpft mit einer einheitlichen und weitgehend standardisierten Plattform.

Die Hosting-Dienstleister können die größte Flexibilität und die interessantesten Preismodelle anbieten, wenn der Kunde IT-Leistungen bezieht, die vom Hosting-Anbieter auf einer Plattform bereitgestellt werden und von mehreren Kunden gemeinsam genutzt werden (Public Utility with Shared Infrastructure).

Vorteile nutzen – Vorsprung realisieren

Bei der Realisierung von NetOpFü und dem gemeinsamen Information Grid stehen Themen wie Flexibilität und Vernetzung von Informationsquellen im Vordergrund. Das führt zu einem Bedarf an einer einheitlichen Architektur; die gilt sowohl auf Systemplattformebene als auch auf Anwendungsebene. Die Zusammenarbeit mit einem Hosting Partner ist eine Variante, die diese Voraussetzungen schaffen kann.

Vorteile für die Bundeswehr

Die Vorteile des Hosting-Ansatzes für die Bundeswehr werden in mehrerlei Hinsicht deutlich:

- Konzentration auf Kernkompetenzen: Bedarfsformulierung an und Nutzung der Aufklärungs-, Führungs- und wirkungsorientierten Systeme durch die Bundeswehr; Umsetzung und Betrieb der IT-Lösungen durch den IT-Partner.

- Erhöhte Flexibilität bei den Kapazitäten variabler IT-Ressourcen. Teilstreitkraftübergreifende Konzeption und Umsetzung ermöglichen Skaleneffekte und flexible Zuordnung der Ressourcen.
- Geringere Komplexität: Eine einheitliche Architektur vereinfacht die Handhabung des gemeinsamen Information Grids und steigert die Flexibilität.
- Optimierung von Verfügbarkeit und Qualität der IT.
- Kostenvariabilisierung und -reduzierung (auch wegen der Übertragung der Assets an den Dienstleister).
- Teilhabe an der marktgetriebenen Innovation. Im Rahmen von NetOpFü sind mit Blick auf mögliche Hosting-Überlegungen folgende Fragen zu beachten.
- Vertraulichkeit der Daten: Inwiefern lässt sich ein solches Vorhaben extern hosten? Der Public Utility-Ansatz (mit gemeinsamer Nutzung der Infrastruktur und/oder Anwendungen durch mehrere Kunden) scheint hierfür unwahrscheinlich. Allerdings liefert die Industrie viele Ansätze, diese Sicherheitsthemen zu lösen, z. B. durch den Einsatz von Verschlüsselungs-, VPN- oder Kryptomechanismen.
- Der teilstreitkraftübergreifende Grid-Ansatz. Der hohe Abstimmungs-, Koordinierungs- und Harmonisierungsbedarf bei einem solchen Ansatz impliziert unvermeidbar einen Bedarf an einer einheitlichen Architektur und Standards. Genau darin liegt die Chance, dies mit einem neutralen Hosting-Partner umzusetzen.

Einsatzbeispiele:
Im Global Information Grid unter starker Beteiligung des US Department of Defense findet der Hosting-Ansatz mehrfach Anwendung.

3.5 Middleware

Informations- und Kommunikationstechnologien – wo wir heute stehen
Middleware bezeichnet in der Informationstechnologie anwendungsunabhängige Technologien, die Dienstleistungen zur Vermittlung zwischen Anwendungen anbieten, so dass die Komplexität der zugrunde liegenden Applikationen und Infrastruktur verborgen wird. Man kann Middleware auch als eine Verteilplattform auf einer höheren Schicht als der gewöhnlichen Rechnerkommunikation auffassen.

Middleware als Dienstleister

Middleware stellt eine Ebene in einem komplexen Software-System dar, die als „Dienstleister“ anderen, ansonsten entkoppelten, Softwarekomponenten die Kommunikation untereinander ermöglicht. Meist erfolgt diese Kommunikation mit Hilfe eines Netzwerkes. Technisch gesehen stellt die Middleware-Software Schnittstellen bzw. Dienste bereit.

Vorteile nutzen – Vorsprung realisieren
Untersuchungen der letzten Jahre haben gezeigt, dass Unternehmen rund 80 Prozent ihres IT-Budgets für Standardgeschäftsabläufe ausgeben und nur 20 Prozent für Bereiche, in denen sie sich wirklich von ihren Wettbewerbern abheben können. Diese Aussage trifft natürlich nicht direkt auf die Bundeswehr zu, da Wettbewerb in diesem Sinne nicht

existiert; die Problematik ist jedoch auch auf die Bundeswehr übertragbar. Die anstehenden Integrationsaufgaben in vielen Projekten, Anwendungen und Produkte in ein gemeinsames System von Geschäftsanwendungen zu integrieren, stellt sich oftmals als schwierig und auch teuer heraus.

Mit geringem Adaptionsaufwand zum Erfolg

Eine mögliche Option besteht in der Arbeit mit einer offenen und flexiblen Kernplattform, die die gesamte Infrastruktur zur Integration vorhandener System, Implementierung neuer Geschäftsabläufe und dynamische Vernetzung von Anwendungen in einer virtuellen Anwendungsumgebung der Bundeswehr bieten können.

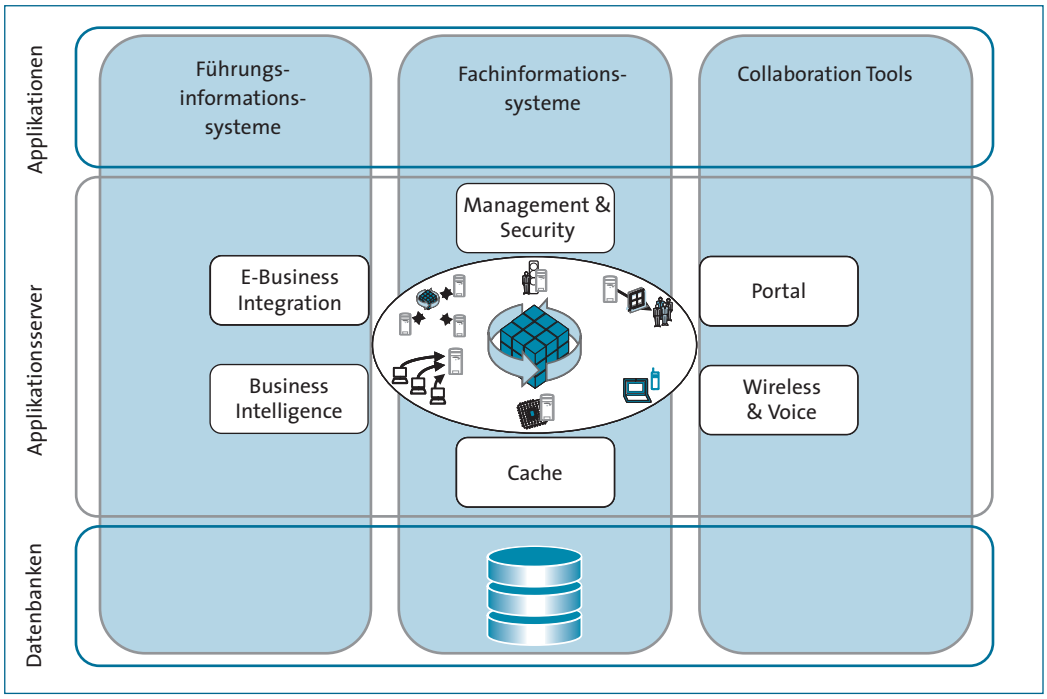


Abbildung 8: Beispiel für eine moderne Drei-Schichten Architektur

Dieses ist weniger aufwendig und beansprucht nur einen geringen Anteil am IT-Budget der Bundeswehr.

Von Vorteilen moderner Middleware profitieren!

Eine moderne Middleware-Architektur hat zum Ziel, der Bundeswehr größere Agilität, bessere Entscheidungen und verringerte Kosten und Risiken mit ihren heterogenen Systemen zu erlauben. Als Teil der Unternehmensinitiative zur einfacheren Integration von Applikationen hilft Middleware, einen umfassenden, offenen und standardbasierten Ansatz für SOA zu schaffen. Mit Hilfe von Web Services, einem Enterprise Service Bus und BPEL zur Implementierung von SOA kann die Bundeswehr problemlos heterogene Geschäftsanwendungen integrieren sowie Geschäftsprozesse automatisieren.

Weitere wesentliche Middleware-Technologien umfassen Technologien für Java-Server, Portal-Lösungen, Integrationskomponenten, Dienste für drahtlosen Zugriff sowie Caching-Technologien.

Java/ J2EE

Moderne Middleware-Technologien umfassen immer auch virtuelle Maschinen für Java. Java2 Enterprise Edition (J2EE) sollte hierbei als Standard-Methodik für das Entwickeln und Betreiben von Enterprise Java Applikationen unterstützt werden. Eine performante, skalierbare und hochverfügbare Basistechnologie ist dabei erforderlich.

Portale

Zu einer modernen Middleware-Architektur zählen Technologien zum Aufbau von Unternehmens-Portalen, beispielsweise Einstiegsportale für Führungsinformationssysteme. Diese bieten dem Anwender einen zentralen Einstieg, lassen sich personalisieren und helfen dem Anwender, die für die jeweilige Rolle passenden Inhalte zu verwalten.

Single Point of Access

Durch die Integration aller relevanten Daten und Applikationen liefert die Portal-Middleware für alle Nutzer einen zentralen Ausgangspunkt.

Personalisierte und rollenbasierte Benutzeroberfläche

Die Portal-Middleware ermöglicht die Berücksichtigung der Rolle des Mitarbeiters und persönlicher Vorlieben im Unternehmen. Diese können individuell, rollenspezifisch und unternehmensspezifisch angepasst werden. Mögliche Rollen: Einkäufer, Controller, Manager, Entwickler, usw.. Das integrierte Single-Sign-On erfordert lediglich eine einmalige Anmeldung mit einem Passwort und danach steht dem Nutzer der Zugriff auf alle seine Anwendungen offen.

Content Management

Durch Content Management wird die Unterstützung unterschiedlicher Arten von Arbeitsabläufe für die Erstellung und Freigabe von Inhalten gewährleistet, ferner die Unterstützung paralleler Teamarbeit und Prozesse durch Check-In und Check-Out von Dokumenten. Ferner wird die automatische Überprüfung interner und externer Links als auch die Versionierung von Inhalten abgedeckt.

Integration

Die heutige IT-Landschaft ist durch ungenügende Integration der Anwendungen gekennzeichnet. Ob es selbstgeschriebene Legacy-Anwendungen sind oder eingekaufte ERP-Anwendungen: alle Lösungen könnten besser miteinander integriert sein. Eine Integration mit externen Partnern mittels automatisierter Geschäftsprozesse ist heute noch die absolute Ausnahme. Zu den Technologien in diesem Bereich zählen Messaging-Systeme, Systeme zur Prozessautomatisierung, Hub&Spoke-Architekturen, BPEL und WebServices.

Wireless

Technologien für drahtlose Anbindung an Portale, Applikationen und Kollaborationskomponenten sollten ebenfalls Teil einer modernen Middleware-Architektur sein. Wireless-Technologien stellen die mobile Ergänzung für Carrier, Portalanbieter, Application Service Provider (ASP) und alle Unternehmen dar, die ihre Mitarbeiter auch unterwegs in ihre elektronischen Geschäftsprozesse integrieren möchten.

Business Intelligence

Business-Intelligence-Funktionalitäten innerhalb von Middleware erlauben die Extraktion und Analyse von Informationen (OLAP) zur Entscheidungsunterstützung. Das intuitive Abfrage-, Berichts- und Analyse-Instrument gewährleistet dem Anwender sofortigen

Zugriff auf jegliche Informationen aus Standard-Datenbanken, Data Marts und Data Warehouses. Um Abfragen, Berichte oder Grafiken zu erstellen oder Datenanalyse zu betreiben, benötigt der Anwender weder Kenntnisse in SQL noch der zugrunde liegenden Datenbankstruktur.

Web Caching

Caching-Technologien ermöglichen, das Antwortzeit-Verhalten von Web Sites und Applikationen zu verbessern. Darüber hinaus reduzieren sie Hardware- und Administrations-Kosten, da sie durch Caching weniger Hardware benötigen, um die gleiche Leistung zu erreichen.

Ein sogenannter Web Cache ist ein RAM-Speicher für statischen und dynamischen Inhalt. Cachen lassen sich unter anderem Servlets, JSP, ASP und weitere Inhalte. Zusätzlich fungiert der Web Cache als Load-Balancer und passt sich nahtlos durch seine Failover Funktionalitäten in ein Gesamt-Verfügbarkeitskonzept ein. Vorteile sind Leistungssteigerungen, Load Balancing und Failover als auch flexible Deployment-Optionen. Ferner erübrigen Invalidierungsmechanismen eine Anpassung an die Anwendungen.

3.6 Informationen und Wissen – Voraussetzung für Wirkung

Die Transformation der Bundeswehr ist Teil eines Veränderungsprozesses in der Gesellschaft, mit dem sich Deutschland den unterschiedlichen Herausforderungen des 21. Jahrhunderts stellt. Für die an diesen Prozessen beteiligten Menschen stellen Neuorientierungen, die Erhöhung der Komplexität und die Prozessgeschwindigkeit erhebliche Herausforderungen dar.

Informations- und Kommunikationstechnologien – wo wir heute stehen
Auch vor dem Hintergrund geringerer finanzieller Ausstattung gewinnt die Auseinandersetzung mit der Qualität dieser Veränderungsprozesse an Bedeutung. Ihre Wirkung entfaltet sich überall dort, wo Menschen zum Einsatz kommen – bei der Ausbildung, in den Führungsstrukturen und den ihnen zuarbeitenden Bereichen sowie beim Einsatz im Feld. Ein wesentlicher Erfolgsgarant für das Management komplexer und dynamischer Prozesse ist die Implementierung von Werkzeugen, die aus der Datenflut entscheidungs- und handlungsrelevante Parameter aufbereiten.

Mit geringem Adaptionsaufwand zum Erfolg
Das Management von Informationen und Wissen bekommt in Gegenwart und Zukunft eine exponential steigende Bedeutung. Komplexität und Beschleunigung von Prozessen sowie die Menge der anfallenden Daten übersteigen das Schrittmaß der menschlichen Entwicklung.

Zudem überfordert die Menge an elektronisch gespeicherten Informationen die menschliche Fähigkeit, allein die Querverweise zu diesen Ablagen zu verwalten. Ferner wird die

Nutzung dieser Ablagen durch eine starke Segmentierung und ihre oftmals nicht NetOpFütaugliche Form stark erschwert. Dadurch kommt es zu einem Widerspruch zwischen der Qualität der Wirkung bei Nutzung der zur Verfügung stehenden Informationen und der im Regelfall zeitkritisch geforderten Leistung. Konventionelle Methoden des Wissens–managements wie die unterschiedlichen Formen der Bereitstellung von Informationen, der zwischenmenschlichen Kommunikation und des konventionellen Lesens müssen durch Technologien zur besseren Aufbereitung des Wissens ergänzt werden, weil sich durch die unaufhörlich wachsende Informationsflut zunehmend Belastungs- und Nutzungsgrenzen aufbauen. Dieses gilt insbesondere für die 90 Prozent an Informationen, die in Form physischer Dokumente existieren.

Anforderung an modernes Wissensmanagement

Insofern ist der Einsatz von Werkzeugen zur besseren Informations- und Wissensversorgung von entscheidender Bedeutung, will man in der Bundeswehr den Transformationsprozess bestmöglich und zeitkritisch erfolgreich bewältigen. Dabei verdienen die folgenden Fähigkeiten eine besondere Beachtung:

- Bewältigung der Informationsmengen und ihrer Nutzung – dezentral, zentral oder extern verfügbare, dynamisch sich entwickelnde oder konsistent verfügbare multimediale Informations- und Wissensbestände effektiv verwalten;
- Infrastrukturen aus Individuen oder Strukturen von Individuen als bereitstellende Träger oder Nutzer von Informationen bestmöglich zu unterstützen und zu versorgen;
- Initiierung und konstante Beibehaltung eines lebenslangen Lernens mit allen Folgen hinsichtlich der Fähigkeiten zur Anpassung an sich ändernde Bedingungen;
- Abbildung von Top-Down-Szenarien auf das Individuum, zum Beispiel bei der Effektivität von miteinander wirkenden Strukturen im Sinne von Netzwerken;
- Umsetzung von Bottom-Up-Szenarien, zum Beispiel bei der Einbeziehung individuellen Wissens und individueller Fähigkeiten innerhalb von Strukturen.

Für die Realisierung dieser Fähigkeiten ergibt sich folgender Bedarf:

- Nutzerfreundliche und hochgradig automatisierte Verwaltung multimedialer Datenbestände wie Papier, E-Mails, Dateien, Internetseiten, Datenbanken;
- Einheitliche und einfach bedienbare Ergonomien;
- Leistungsfähige Suchmechanismen;
- Einfach bedienbare Standardprodukte in Windows-, Client- Server- und WEBkonformen Ergonomien sowie modulare Integrationsfähigkeit sowie komplexen Systemansätzen.

Monolithische Systemansätze werden den verschiedenen Fähigkeiten nicht gerecht werden. Auch in Blick auf eine sich eher evolutionär entwickelnde Systemlandschaft bedarf es ihrer Integration in die Systemumgebungen.

Aufbauend auf allgemeinen informationslogistischen Strukturen lassen sich vielfältige Teilprozesse ableiten, die den allgemeinen Managementprozess von Informationen und Wissen auf den konkreten Bedarf des Nutzers hin weiter qualifizieren. Beispielhaft seien

Ontologien, Push- und Pull- Strategien, Agenten-Technologien und Visualisierung genannt.

Einsatzbeispiele

- Standardsoftware zum Management von Informationen in Dokumenten an jedem Arbeitsplatz.
- Einsatzunterstützung- Informationsräume über dynamisch sich ändernden Infrastrukturen.
- Nachrichtengewinnung, Ausbildungsunterstützung, Qualitätsmanagement.

3.7 Business Intelligence

Informations- und Kommunikationstechnologien – wo wir heute stehen

Business-Intelligence-Software hilft Organisationen dabei, aus ihrem vielfältigen Datenmaterial konkrete Informationen für strategische Entscheidungen zu gewinnen. Mit diesen Lösungen lassen sich Strategien gezielt entwickeln und umsetzen, die eigene Leistungsfähigkeit messen, Kunden- und Lieferantenbeziehungen gestalten und die internen Prozesse analysieren und steuern. Moderne Business-Intelligence-Plattformen gehen über klassisches Data Warehousing und ETL (Extraction, Transformation und Loading) weit hinaus. Sie automatisieren alle Prozesse der Generierung, Verteilung und Anwendung von Wissen. Die Komponenten hinter dieser integrierten Prozesskette umfassen:

Informationsgewinnung für strategische Entscheidungen

1. Datenintegration aus unterschiedlichsten Datenquellen, Formaten, Betriebssystemen und Hardwareplattformen (Datenzugriff, -bereinigung und Metadatenmanagement);
2. Datenmanagement für das Speichern von Daten, für Transparenz und Nachvollziehbarkeit sowie für die Einrichtung einer unternehmensweiten Stammdatenumgebung (Storage, Master Data Management);
3. Datenanalyse für Berichtserstellung, Ad-hoc-Reporting und tiefgehende Analysen (OLAP, Data Mining, Forecasting, Simulationen, GIS-Anbindung);
4. Informationsverteilung für unterschiedliche Nutzergruppen innerhalb der Organisation (Web-Front-Ends, Portale, Analyse-Tools, Integration in vorhandene Office-Anwendungen).

Vorteile nutzen – Vorsprung realisieren

Während operative Systeme keine ausreichende analytische Sicht auf die Prozesse und valide aggregierte Kennzahlen liefern, bieten dispositive Systeme wie Business-Intelligence-Lösungen ein transparentes Bild über alle verteidigungsrelevanten Bereiche einer militärischen Organisation. Sie erhöhen damit die Leistungsfähigkeit der militärischen und zivilen Mitarbeiter.

Mit geringem Adaptionsaufwand zum Erfolg

Laut Aussagen führender Marktforschungsinstitute hat das Thema Business Intelligence für IT-Verantwortliche über alle Branchen hinweg hohe Priorität. Auch im militärischen Bereich kommt Business-Intelligence-Software zunehmend zur Unterstützung der operativen und strategischen Entscheidungsfindung in einzelnen geschäfts- bzw. verteidi-

Business Intelligence als strategischer Faktor zur Transformation der Streitkräfte

gungskritischen Bereichen zum Einsatz. Hier hilft sie, die ambitionierten Ziele hinsichtlich der Kostenoptimierung bei gleichzeitiger Steigerung von Fähigkeiten und Qualität der Aufgabenerfüllung zu erreichen. Business Intelligence ist damit ein strategischer Faktor zur Transformation der Streitkräfte, bei dem folgende Kernaspekte im Vordergrund stehen:

Effizienzgewinn durch Interoperabilität

Interoperabilität. Durch Business-Intelligence-Technologien können von einander unabhängige Systeme weitgehend nahtlos zusammen arbeiten. Dadurch lassen sich Informationen effizient austauschen und den jeweiligen Anwendern und Entscheidern zur Verfügung stellen – ohne Abstimmungsaufwand zwischen den Systemen.

Ausgereifte Datenintegrationsprozesse gewährleisten, dass auch aus völlig heterogenen IT-Landschaften die relevanten Informationen in eine homogene Datenbasis geladen werden. Wichtig sind dabei insbesondere die Datenbereinigung (Data Quality, Master Data Management) und die optimale Datenhaltung für zeitnahe und valide Analysen und Berichterstattung (Realtime). Je nach Informationsbedarf und Anwendungsvorhaben verschiedener Nutzergruppen stellen moderne Systeme zielgruppengerechte Oberflächen bereit und gewährleisten einen weltweiten und mobilen Zugriff.

Effizienzgewinn durch Wissensmanagement

Wissensmanagement. Informationssysteme, die Mitarbeiter vernetzen sowie Informationen sammeln und bereitstellen, fördern die Produktivität einer Organisation. Als Konsequenz haben in den letzten Jahren mehrere Verteidigungsministerien den Arbeitsschwerpunkt Informationsmanagement identifiziert. Die Informationsverarbeitung muss dabei auf die Gesamtstrategie abgestimmt werden.

Einsatzbeispiele

- Führungsunterstützung (Performance Management, z. B. in Form einer Balanced Scorecard oder anderer ganzheitlicher Steuerungssysteme).
- Prozessanalyse und -optimierung (Wirkungsanalyse, Kostentransparenz, Identifikation von Kostentreibern, „Activity-based Management“).
- Finanzmanagement (Haushaltsplanung, -konsolidierung und -budgetierung, Performance-Based Budgeting, Identifikation von möglichem Missbrauch der Mittel).
- Optimierung des Ressourceneinsatzes (Strategische Personalplanung, Rekrutierung & Ausbildung, Materialplanung, Optimierung von Lieferketten und Logistik).
- Simulationen, Szenariomanagement (mit Anbindung von geografischen Informationssystemen).
- Berichtswesen (OLAP-Reporting, Ad-hoc Analysen, Standard- bzw. Massenberichtswesen für Informationskonsolidierung und Wissensmanagement).

3.8 Filtern und semantische Netze

Wissensmanagement durch semantische Netze

Informations- und Kommunikationstechnologien – wo wir heute stehen

Die Anforderungen der Transformation zur rechtzeitigen Bereitstellung von

Informationen machen eine neue Form des Wissensmanagements zur Unterstützung des Faktors Mensch zwingend notwendig. Semantische Netze bieten im Rahmen der Aufarbeitung und Bereitstellung von Informationen dabei enorme Potenziale und stellen einen innovativen Schritt dar, Informationen, sei es für die Recherche und Entscheidungsfindung oder auch für Lernzwecke, in visualisierter Form bereitzustellen. Erst das intelligente Filtering ermöglicht, dass einerseits notwendige Informationen zur Entscheidungsfindung und andererseits komplexe Suchmechanismen für umfangreiche Recherchen in den unterschiedlichsten Datenquellen bereitgestellt werden. Darin lassen sich sowohl syntaktische, semantische aber auch Mustererkennungs-Algorithmen einbinden.

Es handelt es sich um den Aufbau von Informationsstrukturen mit Hilfe von inhaltlichen Beschreibungen. Hierbei werden Informationen semantisch, d. h. hinsichtlich ihrer Bedeutung und ihrer Beziehung zueinander miteinander verknüpft. Im Gegensatz zu der derzeit noch üblichen Volltext- oder Schlagwortsuche in herkömmlichen Wissensmanagement-Umgebungen werden hierbei nach Eingabe eines Suchbegriffes auch solche Dokumente bzw. Themen gefunden, in denen das eingegebene Schlagwort gar nicht vorkommt, damit aber thematisch doch zu tun hat und zur Lösungsfindung beiträgt.

Semantische Netze verfolgen einen zu herkömmlichen Wissensmanagement-Umgebungen komplementären Ansatz. Dieser beinhaltet konkret:
- Bereitstellung und Zugriff auf explizites und implizites Wissen;
- Inhalts- und problemorientierte Suche nach Informationen, Wissen und Wissensträgern;
- Vermeidung von Redundanzen;
- personalisierter Zugriff auf Informations- und Wissensbestände;
- grafische Darstellung von Informationen und Wissen;
- Vermeidung von Informationsüberflutung durch zuständigkeitsbezogene Bereitstellung.

Vorteile nutzen – Vorsprung realisieren
Durch zahlreiche Praxisberichte aus der gewerblichen Wirtschaft ist diese Konzeption die Lösung auf dem Weg zu einem deutlich effizienteren Wissensmanagement, womit sich auch schnell weitere Anknüpfungspunkte an konkrete Möglichkeiten wie zum Beispiel die effiziente Einbindung von arbeitsplatznahen, individualisierten Qualifizierungssystemen (E-Learning) ergeben.

3.9 Visualisierung und ITK-Endgeräte – das Tor zur ITK

Informations- und Kommunikationstechnologien – wo wir heute stehen

Endgeräte: Spitzentechnologie für alle Anforderungen

Die ITK-Endgeräte-Branche ist mit Hardwareherstellern, Software- und Lösungsanbietern sowie Systemintegratoren und Servicefirmen die maßgebliche Basis, um in jedem Geschäftsgebiet relevante Daten zu verarbeiten und Arbeitsschritte zu vereinfachen. Neben klassischen Produkten wie PC-Systemen, Monitoren, Druckern, Servern, Storage-Produkten sowie im mobilen Bereich von PDA-Organizern, Notebooks, Convertible Notebooks und

Pen Tablets entwickelt sich die ITK-Endgeräte-Branche immer mehr zum Lösungspartner. Diese IT-Lösungen garantieren den optimalen Einsatz der Systeme unter Berücksichtigung individueller Kunden-Anforderungen.

Um aus der Vielfalt der technischen Möglichkeiten eine für die eigenen Bedürfnisse passende Lösung zu wählen, benötigt die Bundeswehr IT- Partner, die durch umfassende Beratung eine für den geplanten Einsatz optimierte IT-Lösung zusammenstellen. Diese sollte sich in die bestehende IT-Infrastruktur der Bundeswehr einfügen sowie vorhandene Komponenten und bestehende Programme integrieren.

Vorteile nutzen – Vorsprung realisieren

Standard-Produkte für geeignete Umgebung

Beim Einsatz von Standardprodukten wird der administrative Aufwand auf ein Minimum reduziert, da Software-Installation und Service vereinheitlicht werden. Ein weiterer Vorteil liegt in der konstanten Ersatzteilversorgung. Bei einem nötigen Ersatz einer neuen Komponente für ein Standard-System ist die Wiederbeschaffung oft bis zu fünf Jahren nach Erwerb problemlos. Der Einsatz von jeweils aktuellen Standardprodukten bietet darüber hinaus den einwandfreien Einsatz von neuesten Betriebssystem- und Software-Produkten, für die der aktuelle Standard oft weltweit maßgeblich ist.

Im geschäftskritischen Serverumfeld werden die Standardprodukte in der Regel für Büroanwendungen konzipiert. Der Einsatz dieser Geräte unter extremen Temperaturbedingungen erfordert entsprechende Maßnahmen, wie den Einbau in beispielsweise wassergekühlten Racks oder Containerlösungen mit entsprechenden Anschlüssen, in dem die Systeme transportiert und untergebracht werden. In diesen Containern wird eine konstante Umgebungstemperatur gewährleistet.

Mit geringem Adaptionsaufwand zum Erfolg

Gehärtete Technologien für spezielle Anwendungen

Die Einsatzvielfalt der ITK-Endgeräte setzt für spezielle Anforderungen des militärischen Bereichs eine Konzeption voraus, die über die nichtmilitärischen, meist für Büroumgebungen entwickelten Produkte hinausgeht.

Hier wiederum empfiehlt sich der Einsatz gehärteter Produkte. Sie zeichnen sich durch Ihre Robustheit aus und sind für den Einsatz unter extremen Bedingungen konzipiert.

Im mobilen Bereich, auf „freiem Feld“ und an anderen Einsatzorten, wie z. B. auf See oder in der Luft, werden Daten direkt vor Ort erfasst und können mittels integrierter Funkkommunikation direkt an das Serverumfeld übertragen werden. Dies erspart den doppelten Aufwand des Schreibens und nochmaligen Eingebens dieser Daten in den PC und vermeidet Fehler bereits an der Quelle. Hier bieten sich PDA-Produkte oder Pen-Tablets an.

Um diese Produkte unter Einsatzbedingungen zu schützen, können zwar kratzfeste und wasserdichte Schutztaschen für nicht-robuste Geräte konzipiert werden. Derartige

Lösungen werden allerdings nicht den Härtungsgrad speziell entwickelter Geräte erreichen. Ein Nachteil robuster mobiler Computerlösungen lag allerdings bislang in der Leistungsfähigkeit der Systeme. So konnten abgedichtete Rechner aufgrund der Eigenwärmeentwicklung und Batteriestandzeiten nur langsamere Prozessoren tragen als aktuelle Geräte für den Endverbraucher. Durch aktuelle Notebook-Prozessoren mit minimalem Energieverbrauch und Hitzeentwicklung müssen Nutzer robuster Computer heutzutage nicht mehr auf marktübliche Leistungsmerkmale verzichten.

Trotz marktüblicher Komponenten in solchen Systemen ist das bloße Einsetzen in ein widerstandsfähiges Gehäuse noch kein Garant für optimale Nutzbarkeit und Haltbarkeit im Feld. Gehärtete Computer werden deshalb grundlegend auf die widrigen Umweltbedingungen außerhalb eines Büros gestaltet. Feuchtigkeit, Staub, Hitze, Kälte, Stöße und Vibrationen sind Faktoren, denen Bürorechnern in der Regel nicht ausgesetzt sind. Auch die Integration von Funklösungen oder anderen Erweiterungen kann nicht durch die bloße Verwendung einer kommerziellen Lösung geschehen – offenstehende Klappen oder herausragende Antennen könnten den Ansprüchen an Feldeinsätze nicht genügen. Moderne robuste Mobilcomputer – seien dies Handhelds, Tablet PCs oder Notebooks – bieten neben der Zuverlässigkeit auch marktübliche Komponenten und Zubehör, das auf den wirklich mobilen Einsatz zugeschnitten ist (Tragelösungen, Fahrzeughalterungen etc.). Kombiniert mit Produktlebenszyklen, die eine Kompatibilität von Zubehör und einen Investitionsschutz garantieren, sind robuste Systeme unumgänglich, wenn es um missionskritische Projekte geht.

Einsatzbeispiele

Pen Tablets: Im mobilen Einsatz unterwegs können die Daten direkt über das System erfasst werden. Bei einer entsprechenden WLAN-/Netz-Verbindung und Softwarelösung werden die Daten direkt auf dem entsprechenden Server gespeichert.

Des Weiteren gibt es verschiedene Möglichkeiten, um mit nur einem Eingabeschritt die Daten direkt auf dem Server zu speichern und diese über Storage-Systeme zu verwalten (zum Beispiel Thin Client in Verbindung mit Servern). Die Verwaltung sowie das Bearbeiten aller Unternehmensdaten und Programme erfolgen zentral auf dem Server. Der PC ist in diesem Fall lediglich das Ein- und Ausgabeinstrument. Der Administrationsaufwand ist für diese Lösung minimal, da alle Installationen und Software-Updates lediglich auf dem Server getätigt werden müssen. Die Zugriffsrechte können je User individuell eingestellt werden.

Virtuelles Magnetband-Bibliotheksystem. Um den hohen Administrationsaufwand aufgrund des Einsatzes von unterschiedlichen Serverplattformen und Datensicherungslösungen sowie der hohen Kapazitäten der Magnetbänder zu minimieren, kann eine Backup-Virtualisierung umfassende Abhilfe schaffen. Diese „Hardware-Lösung“ bietet einen plattformunabhängigen Schutz der Daten mit nahtloser Integration in nahezu jede

existierende IT-Umgebung. Die umfassende Konnektivität erlaubt den Unternehmen die Konsolidierung der gesamten Bandbreite heutiger Magnetbandsysteme in Systemumgebungen von offenen Systemen und Mainframes. Den angeschlossenen Servern und Backup-Applikationen wird im Storage Area Network über virtuelle Bandlaufwerke eine Vielzahl ständig verfügbarer und hochleistungsfähiger Ressourcen für das Backup und Restore angeboten.

Technologien und Lösungen zur Realisierung einer dynamischen und serviceorientierten Architektur. Basis bilden hierbei virtualisierte und verteilte Ressourcen, die je nach Bedarf und Priorität den anfordernden Prozessen zugewiesen werden können. Wichtige Leistungswerte sind hierbei Unterstützung von 1:n-Failover- Szenarien, schnelle Interconnect-Zeiten zwischen den virtualisierten Systemen und die Konsolidierung der physikalisch zu realisierenden Infrastruktur-Schnittstellen. Bei der Realisierung von Compute-Nodes werden hardwarenahe Virtualisierungstechnologien zur effizienten Ausnutzung der Ressourcen präferiert. Unterstützt werden müssen solche Technologien durch ein abgestuftes Berechtigungskonzept zur Administration der Gesamtlösung.

4 Betrieb der Matrix

4.1 Sicherer Verkehr im Netz: Kryptographie und Kommunikation

Die aktuellen und zukünftigen Aufgaben der Streitkräfte führen zu ständig wachsenden Anforderungen an die militärischen Kommunikationsmöglichkeiten. Die Entwicklung und Anwendung neuer Kommando- und Führungssysteme ist zunehmend mit höheren Datenübertragungsraten und mit modernen Technologien wie TCP/IP oder Satellitenkommunikation verbunden. In diesem Kontext sind zuverlässige, sichere und schnelle Kommunikationsverbindungen unter Einsatzbedingungen entscheidend. Die Sprach-, Video- und Datennetzwerke mit ihren technischen Komponenten sind dabei durch geeignete Maßnahmen zu schützen, damit gegnerische Aufklärer möglichst keine Informationen über die eingesetzten Kräfte, Ausrüstungen, Vorhaben und eventuelle Schwachstellen ableiten können. Dies betrifft sowohl den Übungs- als auch den Einsatzfall.

Informations- und Kommunikationstechnologien – wo wir heute stehen

Ziel: Erhöhung der Kommunikationssicherheit

Ein wesentlicher Bestandteil sind hierbei Maßnahmen zur Erhöhung der Kommunikationssicherheit (COMSEC), d. h. Maßnahmen zur Verhinderung der Kenntnisnahme der übertragenen Informationen durch Unbefugte und zur Sicherung der Authentizität und Integrität der übertragenen Informationen. Zu COMSEC gehören:

- Kryptosicherheit (Einsatz und korrekte Anwendung geeigneter Kryptosysteme);
- Physische Sicherheit (physische Maßnahmen zur Sicherung der Kommunikationssysteme);
- Übertragungssicherheit (Transmission Security = TRANSEC; Maßnahmen zum Schutz der Übertragungen gegen Abhören und Manipulationen zusätzlich zum Einsatz von Kryptosystemen);
- Emissionssicherheit (Schutz gegen das Abfangen kompromittierender Abstrahlung).

Im Folgenden werden einige Fragen der Kryptosicherheit behandelt.

Das traditionelle Hauptziel der Kryptographie-Anwendung besteht in der Wahrung der Vertraulichkeit von Informationen mittels Verschlüsselung. Als andere wichtige Anwendungsfelder bildeten sich die Überprüfbarkeit der Authentizität und Integrität von Informationen (z. B. durch Prüfung digitaler Signaturen) sowie die zuverlässige Identifizierung/Authentisierung von Kommunikationsteilnehmern heraus.

Vorteile nutzen – Vorsprung realisieren

Die moderne Kryptographie umfasst ein breites Spektrum von Verfahren, die zum Teil auf komplizierten mathematischen Theorien beruhen. In ähnlichem Maße entstanden auch immer bessere Methoden zur Analyse dieser Verfahren. Insofern hat sich hier ein ständiger Wettlauf entwickelt, bei dem gegenwärtig aber ein Übergewicht für die Entwickler

vorliegen dürfte. Das heißt, es gibt gründlich untersuchte kryptographische Methoden, die bei richtiger Anwendung ein hohes Maß an Sicherheit bieten.

Die Verschlüsselung beinhaltet die umkehrbare Umformung der Darstellung einer Information (des Klartextes) in eine andere Darstellung (den Geheimtext) mit dem Ziel der Geheimhaltung der Informationsinhalte. Dazu wird im Allgemeinen ein geheimer Parameter (Schlüssel) genutzt (oder mehrere), der die erwähnte Umformung wesentlich beeinflusst. Im Prinzip wird hier die Geheimhaltung der Informationsinhalte auf die Geheimhaltung des Schlüssels reduziert. Die Geheimhaltung der Umformungsregeln (d. h. des Kryptoalgorithmus) kann, soweit überhaupt möglich, (zumindest zeitweise) zusätzliche Sicherheit bewirken.

Stromchiffren

Bei Stromchiffren wird der Klartext als Bitstrom betrachtet. Aus einem Schlüssel und (zumeist) einem Anfangswert wird eine zufällig aussehende Bitfolge erzeugt, die dann bitweise mit den Klartextbits verknüpft wird. Zur Entschlüsselung wird die gleiche zufällig aussehende Bitfolge erzeugt, um die Verknüpfung dann rückgängig zu machen. Bekannte Beispiele aus dem zivilen Umfeld sind der RC4, der in vielen Softwareprodukten verwendet wird, der A5 (in jedem GSM-Handy) und der E0 (in Bluetooth-Produkten).

Blockchiffren

Blockchiffren formen den Klartext mittels komplizierter blockweiser (zumeist in Blöcken von 64 Bit oder 128 Bit) schlüsselabhängiger Transformationen um. Auch hier gibt es bekannte Vertreter: der Data Encryption Standard DES (seit einigen Jahren wegen der zu kurzen Schlüssellänge nicht mehr ausreichend sicher), der International Data Encryption Algorithm IDEA und Rijndael, der inzwischen als Advanced Encryption Standard AES standardisiert ist und weltweite Verbreitung gefunden hat.

Asymmetrische Krypto-Verfahren

Asymmetrische Krypto-Verfahren sind seit den 1970er Jahren bekannt. Sie werden oftmals dazu genutzt, die geheimen Schlüssel der bereits erwähnten Verschlüsselungsmethoden sicher zu verwalten, d. h. sicher zu vereinbaren, sicher zu verteilen oder einfach zu schützen. Hinzu kommt ein weiter zunehmender Einsatz solcher Verfahren zur Berechnung und Prüfung digitaler Signaturen. Am weitesten verbreitet ist das RSA-Verfahren. In den letzten Jahren wurden jedoch bestimmte Vorteile von Verfahren auf Basis elliptischer Kurven (vor allem kürzere Schlüssellängen bei annähernd gleichem Sicherheitsniveau) deutlich, so dass eine weitere Zunahme des Anteils von Anwendungen dieser Verfahren zu erwarten ist. Die Schlüsselvereinbarung nach der Diffie-Hellman-Methode kann ebenfalls auf Basis elliptischer Kurven realisiert werden.

Kryptoverfahren im Kontext der IT-Sicherheit

Mit geringem Adaptionsaufwand zum Erfolg

Kryptoverfahren leisten, auch wenn sie als sicher gelten, aber nur dann einen wesentlichen Beitrag zur Erhöhung der Informations- und Kommunikationssicherheit, wenn sie korrekt implementiert und angewendet werden. Insbesondere bildet die sichere Verteilung und Verwahrung der geheimen Schlüssel eine grundlegende Voraussetzung.

Auch ein kryptographisch starker Verschlüsselungsalgorithmus nutzt nichts, wenn z. B. der zur Entschlüsselung erforderliche Schlüssel ein Geheimnis mehr ist. Daher ist es wichtig, zur Erhöhung der IT-Sicherheit professionell entwickelte Produkte und die dazugehörigen Security-Managementsysteme einzusetzen und die Anwendungsbedingungen entsprechend zu berücksichtigen.

4.2 Sicherheit im Betrieb

Informations- und Kommunikationstechnologien – wo wir heute stehen
Im COTS-Bereich sind Anwendungen, Rechnerplattformen und -Architekturen mittlerweile von einer weitgehenden Modularität gekennzeichnet. Die Module wiederum arbeiten über Industriestandards zusammen. Daher ist es heute leicht, kommerzielle Module durch militärischen Anforderungen entsprechende zu ersetzen und somit den Aufwand für spezielle Entwicklungen zu sparen bzw. für die Anpassung an militärische Anforderungen zu minimieren.

Die zunehmende Nutzung von IT-Netzwerken ist eine – keinesfalls neue – Entwicklung, welche sowohl in zivilen als auch in militärischen Anwendungsgebieten stattfindet. Beide Bereiche verwenden im Wesentlichen sehr ähnliche Systeme, welche aber wiederum durchaus unterschiedlichen Policies unterliegen. Vertrauenswürdiger Einsatz und Betrieb von IT-Infrastrukturen erfordert sichere Systeme und insbesondere ein umfassendes Management von Betriebs- und Sicherheitsrisiken.

Vorteile nutzen – Vorsprung realisieren

IT-Sicherheit: Erhöhte Anforderungen im militärischen Bereich

Speziell die IT-Sicherheit ist hierbei derjenige Aspekt, welcher die Bereiche „zivil“ und „militärisch“ unterscheidet. In der Regel sind daher im militärischen Bereich immer vergleichsweise anspruchsvollere Anforderungen im Rahmen der Policies anzutreffen, während die zugrunde liegende Technik eher dieselbe ist. Um eine adäquate Sicherheit im Betrieb zu erreichen, können COTS-Produkte durchaus diesen erhöhten Sicherheitsanforderungen angepasst werden, bzw. können diese erhöhten Anforderungen durch Zusammenschaltung von Standardkomponenten erfüllt werden, ohne Änderungen an den Standardlösungen zu erfordern.

Damit ergeben sich aus der Verwendung von COTS-Lösungen die folgenden Vorteile für den militärischen Betrieb:

- Schnelle Verfügbarkeit;
- Kein, geringer oder allenfalls mäßiger Anpassungsaufwand;
- In der Regel niedrige Beschaffungskosten;
- In einem wesentlich größerem Markt eingeführte Qualität;
- Volle Nutzung des industriellen Innovationspotenzials;
- Schnellere Aktualisierung und Fehlerbehebung;
- Wartung als externe Dienstleistung ohne eigenen Personalaufwand.

Mit geringem Adaptionsaufwand zum Erfolg

Der sichere Betrieb eines IT-Netzwerks, der entsprechenden Middleware und der Endgeräte muss die Aspekte Management (Netzwerk, Security, Policy), Netzwerksicherheit (Firewalls, VPN, Verschlüsselung, Anti-Virus, Intrusion Detection) und sichere Endgeräte (Thin Clients, Workstations, Server, Zugriffskontrolle, lokale Verschlüsselung) abdecken.

Militärische und zivile Ansätze – oft komplementär

Standardisierte Ansätze für das Management von Sicherheit im IT-Betrieb in militärischen und zivilen Bereichen können durchaus komplementär sein. Anforderungen aus militärischen Standards können mit Hilfe bewährter Vorgaben für Sicherheits-Management (z. B. Security Management Prozess in ITIL, BS15000, ISO 17799, ISO 27001) kombiniert und in entsprechende Policies und Lösungen entwickelt werden. Adressierte Themen sind Dokumentation der Verfahren und Infrastrukturen, definierte Prozesse für Incident Management, Schulung und Awareness der Operateure.

Zudem hat sich ein 3-stufiges Konzept zur Überprüfung der Einhaltung dieser Maßnahmen bewährt, das auf gängigen Standards basieren kann bzw. sich mehrere zu Nutzen macht (zum Beispiel ITIL, ISO27001, Cobit):

- Self Assessments (werden meist von den Prozessbeteiligten selbst durchgeführt);
- Interne Audits (von internen IT-Sicherheits-Auditoren durchgeführt);
- Externe Audits (von externen IT-Sicherheits-Auditoren durchgeführt; Möglichkeit zur Zertifizierung nach z. B. BSI-Grundschutz, ISO27001).

Einsatzbeispiele

Die Netzwerksicherheit beruht grundsätzlich auf dem Einsatz kommerzieller Anwendungen, deren Konfiguration einer militärischen Policy entspricht. Eine Ausnahme hiervon sind die Verschlüsselungsgeräte, die IPsec-konform sind (der wiederum ein kommerzieller Standard ist), dafür aber nur zugelassene Algorithmen verwenden.

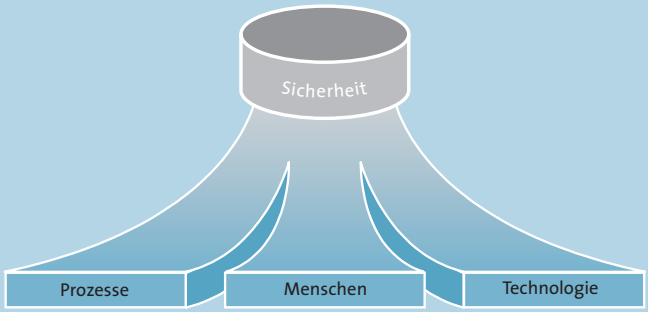
Beispiele:

- IP-Verschlüsselung
- Boundary Protection Devices
- Internet Exchange Gateways

Sichere Endgeräte sind z. B. gehärtete Industrie-PCs, welche über ein entsprechendes „ruggedized“ Gehäuse, ein geprüftes Betriebssystem und zugriffskontrollierte Schnittstellen sowie Anwendungen verfügen.

Ein Beispiel hierfür ist die Virtual Workstation, die basierend auf einem Industrie-PC mit einem gehärteten kommerziellen Betriebssystem eine sichere Plattform für beliebige Anwendungen darstellt. Die VW kapselt in einer Virtual Machine ein weiteres, frei wählbares und natürlich auch kommerzielles Betriebssystem, welches dem User für alle Anwendungen zur Verfügung steht. Zugriff auf Ressourcen und Netzwerkverbindungen werden über Smart Cards verwaltet.

Grundsätzlich wird so für eine homogene Integration der Sicherheitsanforderungen (definiert in entsprechenden Policies) in allen drei Säulen der IT gesorgt: Menschen, Prozesse und Technik.



4.3 Risikomanagement

Informations- und Kommunikationstechnologien – wo wir heute stehen
Die Öffnung und Globalisierung von Märkten und die zunehmende Vernetzung von Systemen und Organisationen ziehen naturgemäß auch die Notwendigkeit verstärkter Regulierung und vertraglicher Verpflichtungen zwischen den Partnern nach sich. Unternehmen werden damit vor die Herausforderung der Aufstellung und Sicherstellung von übergreifenden Risikomanagementstrategien gestellt.

Vorteile nutzen – Vorsprung realisieren
ERM (Enterprise Risk Management) wird definiert als ein kontinuierlicher, ständig zu optimierender Prozess zur Herstellung hinreichender Sicherheit und Vertrauens hinsichtlich der organisationsspezifischen Zielerfüllung durch die Anwendung einer Strategie auf alle Ebenen der Belegschaft und alle Bereiche der Organisation, die Identifikation von Einflussparametern sowie die Einhaltung einer vorab definierten – und begrenzten – Risikobereitschaft.

Risikomanagement als strategische Führungsaufgabe

Risikomanagement etabliert sich zunehmend als Aufgabe der strategischen Unternehmensführung; der ITK kommt damit in zunehmend vernetzten Umgebungen verstärkte Bedeutung zu. Etablierten Marktforschungsinstituten zufolge sind 82 % der IT-Sicherheits- und Datenschutzaufwendungen im vergangenen Jahr im Zusammenhang mit der Entwicklung von ERM-Strategien und Implementierungen zu sehen.

Verstärkt entwickelt sich die Informationstechnologie zum ERM-Befähiger – durch Automation der Risikomanagement- und Risikobemessungsprozesse, unter anderem auf Basis von Modellbildung und vorausschauender Simulation.

Mit geringem Adaptionsaufwand zum Erfolg

Risikomanagement als Teil von EBO

Zielerfüllung für die Bundeswehr ist die Befähigung zu Effekte erzielender Einsatzführung (Effects Based Planning & Operations, EBO). Risikomanagement umfasst daher insbeson-

dere die möglichst effiziente Optimierung gewünschter und Minimierung unerwünschter (Neben-) Effekte.

ITK als Basis von Risikomanagement

Ein stringentes IT-Sicherheits- und Risikomanagement im NetOpFü ermöglichenden und unterstützenden IT-System der Bundeswehr im gesamten Sicherheitszyklus ist für die erfolgreiche Umsetzung der Konzepte in Führungsinformationssystemen unabdingbar.

Die IT-seitige Umsetzung dieses Zyklus beruht auf den nachfolgende Technologiefeldern:

- Überwachung durch intelligente, autarke Sensoren inner- und außerhalb der Komponenten und Teilsysteme;
- Automation auf Basis von Regelwerken, Metriken, Referenzmodellen, Mustererkennung;
- Identitäts- und Zugriffsmanagement;
- Konformitätsmanagement.

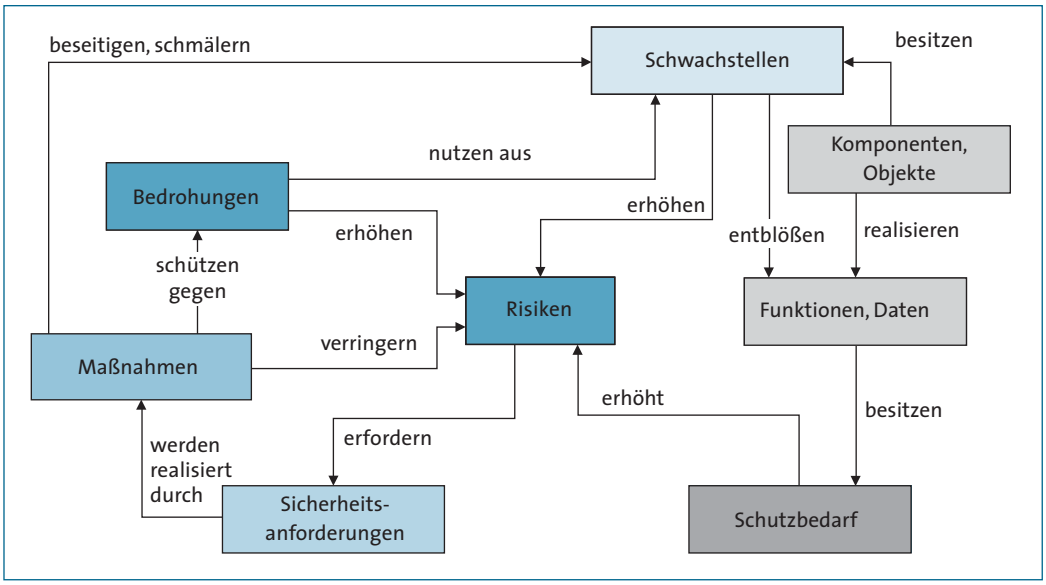


Abbildung 9: Risikomanagement im Kreislauf

Mit erhöhter Komplexität derartiger IT-Infrastrukturen steigt auch die Nachfrage nach IT-Sicherheitsspezialisten. Die deutsche ITK-Wirtschaft bietet eine umfangreiche Palette von Werkzeugen, Lösungen und Dienstleistungen für eine stets aktuelle Inventarisierung und Überwachung aller betriebenen IT-Systeme sowie von Netzwerksicherungslösungen wie z. B. Screens, Proxies, Firewalls, Intrusion Detection Systeme. Im Rahmen einer Public-Private-Partnerschaft (PPP) von Wirtschaft, Forschung und Bundeswehr könnte damit eine „Sicherheitsleitzentrale“ (CERT) mit folgenden Fähigkeiten aufgebaut werden:

- Alarmierung. Während oder nach einem Vorfall muss ein adäquater Adressatenkreis über Ereignis und Auswirkungen automatisch informiert werden.
- Warnung. Aktuelle Situationen werden bewertet und proaktive Prognosen erstellt.
- Reaktion (Schadensbegrenzung, Ursachenforschung, Gegenmaßnahmen, Wiederherstellung des Normalzustands).

5 Von technologischen Spitzenleistungen in Deutschland zur Interoperabilität im Bündnis

Informations- und Kommunikationstechnologien – wo wir heute stehen
Die deutsche ITK-Wirtschaft mit ihrem erworbenen Know-How und ihren Produkten ist in der Lage, die permanenten Veränderungen der Standards rechtzeitig für die Bundeswehr zu adaptieren und stellt somit sicher, dass Streitkräfte jederzeit auf Basis der vorgegebenen Standards im Bündnis kommunizieren können. Die Nutzung von Standardsoftware, wie zum Beispiel zukunftsweisende Integrationsplattformen und Messagingsysteme, gewährleisten stets ein richtiges Schnittstellenmanagement für die gegebenen Standards. Auch sind heutige Middlewaresysteme in der Lage, unterschiedliche Standards automatisiert miteinander zu verbinden.

Ein weiterer wesentlicher Aspekt ist die Integration. In der Dynamik weltweiter Einsatzszenarien ergeben sich Notwendigkeiten zur Interaktion zwischen Systemen, bei deren Entwicklung keine Anforderungen zur Interaktion mit andersartigen Systemen bzw. entsprechenden Systemen anderer Nationen bekannt waren. Auch müssen Systeme der gleichen Anwendungsdomäne zusammenarbeiten, die verschiedene Standards (z. B. ADatP-3 und OTH-G) oder unterschiedliche Versionen bzw. Baselines eines gleichen Standards nutzen. Auch können durch die Integration mehrerer einzelner Systeme aus verschiedenen Domänen Synergien erzielt werden.

Vorteile nutzen – Vorsprung realisieren

Interoperabilittät im Kontext der NATO

Interoperabilität wird von der NATO als „ability to operate in synergy in the execution of assigned tasks" definiert. Interoperabilität ist die Fähigkeit von Systemen, Informationen auszutauschen und so zu verarbeiten, dass eine wirksame Zusammenarbeit gewährleistet ist.

- Technische Interoperabilität ist gegeben, wenn die physikalischen und technischen Merkmale zum Datenaustausch genau erfüllt werden.
- Prozedurale Interoperabilität liegt vor, wenn die Form der Daten (z. B. Meldungsformate) sowie die Betriebsverfahren übereinstimmen.
- Operationelle Interoperabilität setzt einheitliche Einsatzgrundsätze, verbindliche Verfahren, eindeutige Begriffe, sowie abgestimmte Forderungen und Erwartungen an den Informationsaustausch voraus.

Die Fähigkeit zur Zusammenarbeit in militärischen Systemen geht dabei weit über die rein technische Interoperabilität hinaus. Sie schließt prozedurale und operationelle Interoperabilität mit ein.

Interoperabilität im Bündnis ist auf verschiedenen Ebenen angesiedelt:

- Interoperabilität von Streitkräften in einem multinationalen Umfeld insgesamt.

- Interoperabilität von Systemen der verschiedenen Streitkräfte (Waffen-, IT- oder andere Systeme).
- Interoperabilität
  - zwischen nationalen Systemen und Systemen der NATO;
  - zwischen Systemen verschiedener Nationen untereinander;
  - zwischen verschiedenen Systemen einer Nation.

Die Anforderungen nach Interoperabilität betreffen damit die Gesamtheit des IT-Systems der Streitkräfte.

Interoperabilität und Standardisierung

Eng verknüpft mit Interoperabilität ist der Begriff Standardisierung. Erst die Vereinbarung gemeinsamer Begriffe, sowie die verbindliche Festlegungen technischer Merkmale, Formate und Verfahren, die sich in Standards und ggf. auch Normen niederschlagen, schaffen die Voraussetzungen für Interoperabilität zwischen Systemen.

Neben der Nutzung internationaler Standards von Organisationen wie z. B. der ISO (International Standardization Organsiation) werden auf Ebene der NATO eigene Festlegungen im Rahmen von Standardisation Agreements (STANAGs) getroffen. Diese Standards sind meist sehr umfangreich und werden in Systemen selten in ihrem vollen Umfang genutzt oder für die Interaktion mit anderen Systemen benötigt. Daher wurden spezielle Programme aufgelegt, die Interoperabilität zwischen Führungsinformationssystemen auf Basis einer für ein bestimmtes Einsatzumfeld relevante Untermenge eines Standards erreichen sollten (QIP / BIP). Mit veränderten politischen Randbedingungen sind diese Aktivitäten nicht länger auf die NATO beschränkt.

Standards treffen Festlegungen für den Umgang mit Objekten der realen Welt. Sie müssen ständig den sich veränderten Anforderungen und Randbedingungen entsprechend angepasst werden und unterliegen damit einem Lebenszyklus, der an den der abgebildeten Objekte angelehnt ist. Die Fortschreibung erzeugt neue Stände oder Versionen, die oft übergreifend in sog. Baselines festgeschrieben werden.

Damit Systeme interoperabel agieren können, ist es notwendig, jeweils für bestimmte Zeiträume verbindlich festzulegen, welche Versionen oder Baselines der zugrunde liegenden Standards genutzt werden – bis veränderte Umgebungsbedingungen den Umstieg auf Weiterentwicklungen erforderlich machen.

Interaktion von Systemen in einem dynamischen Umfeld

Weder eine kurzfristige Anpassung oder Erweiterung betroffener Systeme noch eine umfassende Anpassung aller genutzten Systeme an sich ständig verändernde Randbedingungen sind finanziell noch anderweitig unter dem Gesichtspunkt knapper Ressourcen leistbar – und notwendig. Hier können entsprechend flexible Technologien für die Integration helfen, Interaktion zwischen Systemen (auch kurzfristig) herzustellen. Auf Basis einer derartigen Integrationsplattform können – soweit die verfügbaren Schnittstellen

fachlich die jeweils notwendigen Informationen bereitstellen – Interaktionen zwischen Systemen mit Anpassungen von Datenformaten und Übertragungsprotokollen geschaffen werden, ohne die jeweiligen eingeführten Systeme selbst anzupassen.

Auf Basis des Know-Hows der Anwendungsdomänen und der genutzten Standards wird hiermit die Grundlage für sanfte Migrationen auf der Basis veränderter Anforderungen geschaffen.

ITK: Fundament der Interoparabilität im Bündnis!

Leistungsfähige Integrationsplattformen, wie sie heutzutage auf dem ITK-Markt verfügbar sind, werden diesen komplexen Anforderungen gerecht. Sie führen Menschen, Informationen und Prozesse zusammen – über alle organisatorischen Grenzen hinweg – und integrieren Informationen und Anwendungen aus verschiedensten Quellen. Sie eignen sich als Fundament für Interoperabilität im Bündnis für die Zukunft.

6 Thinking ahead – Beitrag der deutschen ITK-Wirtschaft zur Technologiesicherung am Standort

Sicherung der Technologieführerschaft am Standort Deutschland bedeutet zweierlei: Einerseits die vorausschauende Investition in Forschung und Entwicklung, um mit dem technologischen Stand im internationalen Kontext Schritt zu halten. Andererseits sollte die Möglichkeit genutzt werden, in einer Simulations- und Testumgebung Flexibilität und Leistungsfähigkeit neuer Lösungen zu testen und damit deren schnelle Zuführung in den Einsatz zu ermöglichen.

6.1 Forschung und Technologie

Informations- und Kommunikationstechnologien – wo wir heute stehen
Forschung und Entwicklung gehören zu den Kernaktivitäten einer Branche, deren Anspruch darin besteht, zu den innovativsten Wirtschaftszweigen zu gehören. Der Anteil der F&E-Ausgaben am Bruttoinlandsprodukt beträgt allerdings weiterhin nur 2,5% in Deutschland. Zur Sicherung technologischer Spitzenleistungen sind F&E-Mittel zu stärken, dazu gehört auch der Ausbau der Wehrforschung, wehrtechnischen und sonstigen militärischen Entwicklung und Erprobung.

Vorteile nutzen – Vorsprung realisieren
In der Vergangenheit mussten unter dem Grundsatz der Erfüllung der Aufgaben der Bundeswehr als Verteidigungsarmee eine Fülle von neuen technologischen Herausforderungen auch und vor allem in der ITK-Unterstützung gelöst werden. Unter dem Zwang, ressourcensparende und möglichst schlanke, dem militärischen Einsatz optimal angepasste Lösungen bereit zu stellen, sind vielfältige Anstrengungen in Forschungs- und Entwicklungsvorhaben unternommen worden, deren Ergebnis über Jahrzehnte gewachsene, für einen dezidierten Zweck optimierte Speziallösungen waren.

Technologieintegration durch F&T Verstärkung stützen!

Die politischen Vorgaben für die Bundeswehr haben sich indes gewandelt: die Bundeswehr entwickelt sich von einer Verteidigungsarmee rasant zu einer Einsatzarmee. Einhergehend mit den veränderten Anforderungen und den Zwängen der Haushaltskonsolidierung müssen auch die bundeswehrinternen Prozesse zu Forschung und Technologie angepasst werden. Auch wenn die Bundeswehr zur Zeit nur begrenzt die Möglichkeit hat, Forschungsvorhaben ergänzend zu den Maßnahmen der zivilen Ministerien zu planen, müssen verstärkt Anstrengungen unternommen werden, die größer werdende Kluft zwischen Ausrüstungsstand der Bundeswehr und Einsatzanforderungen wieder zu schließen. Dies setzt innovative Lösungen voraus, die auf marktkonformen Produkten und Lösungen basieren und mit möglichst effektivem Einsatz der verfügbaren Mittel auf die Anforderungen der Bundeswehr adaptiert werden können.

Dabei sind sowohl die Zeit als auch die zur Verfügung stehenden Mittel für die Grundlagenforschung im militärischen Bereich begrenzt, so dass bereits angestoßene Forschungsaktivitäten der zivilen Industrie verstärkt sowie mit Hilfe der industriellen Erfahrung in neue Gebiete vorgestoßen werden sollte. Der Vorteil für die Bundeswehr bei einer intensivierten Investition in F&E-Integration an der Schnittstelle des militärischen und zivilen Bereichs liegt auf der Hand:

Wettbewerb im zivilen Markt als Garant der Technologiesicherung im militärischen Umfeld

Unter dem Druck der ständig steigenden Kundenanforderungen und aufgrund des weltweiten, nahezu uneingeschränkten Wettbewerbs im zivilen Markt werden die ITK-Unternehmen gezwungen, sich und ihre Produkte und Lösungen fortlaufend weiter zu entwickeln. Eine „unnütze“ und ggf. nur den Eigeninteressen eines Unternehmens dienende Produktpalette wird alleine schon durch die Heterogenität des Marktes und das Fehlen steuernder Autoritäten und den damit verbundenen Zwang zur Interoperabilität verhindert. Insofern investiert die ITK-Wirtschaft konsequent und unter Einsatz von hohen personellen und finanziellen Ressourcen in die Forschung, um sich im stetig verändernden weltweiten Markt behaupten zu können.

Mit geringem Adaptionsaufwand zum Erfolg

Dies wird erreicht durch Maßnahmen der Forschung und Technologie, die u. a. folgende Elemente verstärkt erfassen sollten:

- Erprobung marktgängiger Produkte (COTS) mit dem Ziel, die Zeiträume bis zur Marktverfügbarkeit von neuen Produkten durch preiswerte Adaptionen von verfügbaren Technologien und Produkten zu überbrücken;
- Verifikation der Forderungserfüllung durch Simulation und Einsätze in Testzentren sowie in separierten Probeszenarien;
- Erstellung von Konzeptstudien zur Validierung einer Einsatzreife in Szenarien der Bundeswehr.

Diese F&E-Maßnahmen sind logisch mit CD&E zu koppeln, um das nahtlose Zusammenspiel von Technologien im Transformationsprozess der Bundeswehr zu gewährleisten.

6.2 Simulations- und Testumgebung

Informations- und Kommunikationstechnologien – wo wir heute stehen

Die Simulations- und Testumgebung der Bundeswehr (SuT Bw) bildet im Transformationsprozess der Bundeswehr den technischen Rahmen, um reale und simulierte Systeme in verteilter Umgebung, direkt oder indirekt miteinander zu vernetzen. Bei Bedarf können gewonnene Informationen analysiert und bewertet werden, um Erkenntnisse für das weitere Vorgehen zu gewinnen.

S&T: Ein vielseitiges Instrument für ein breites Aufgabespektrum

Dabei bildet die SuT Bw die Werkbank des Transformationsprozesses der Bundeswehr und kann in folgenden Anwendungsfeldern zum Einsatz kommen:

- Anwendung der Methode Concept Development and Experimentation (CD&E);

- Bedarfsermittlung, Bedarfsdeckung und Nutzung im Rahmen des Customer Product Management (CPM);
- Ausbildung und Durchführung von Übungen;
- Analyse und Planung;
- Vorbereitung, Durchführung und Nachbereitung von Einsätzen.

In Abhängigkeit des Anwendungszwecks werden auf die SuT Bw administrativ-organisatorische Umgebungen aufgesetzt. Ein Beispiel hierfür ist der Verbund Modellbildung und Simulation (M&S-Verbund Bw), der in der Teilkonzeption Modellbildung und Simulation Bundeswehr festgelegt worden ist. Die SuT Bw muss folglich für ein breites Nutzerspektrum konzipiert sein und für die jeweilige Aufgabe ein hohes Maß an Anpassungsfähigkeit bieten. Flexibilität und Leistungsfähigkeit sind von grundlegender Bedeutung.

S&T: Ein Ansatz zur Integration vorhandener Technologien

Vorteile nutzen – Vorsprung realisieren

Die technische Architektur der SuT Bw kann als Drei-Ebenen-System zur Kopplung von Simulationssystemen und technischen Einzelkomponenten verstanden werden. Physikalisch setzt sie auf ein vorhandenes Netzwerk wie zum Beispiel das Kommunikationssystem der Bundeswehr oder zivile Telefon- und Datennetze auf. Im Rahmen von Experimenten werden Verbünde geschlossen, die es erlauben, Untersuchungen und Analysen in den Anwendungsfeldern der SuT Bw durchzuführen. Hierzu werden die bereitgestellten Dienste und Werkzeuge, sowie bei Bedarf zusätzlich notwendige Hard- und Software genutzt. Typische Anwendungen der SuT Bw können Simulationssysteme und Simulatoren, aber auch Führungsinformations- und einzelne Waffensysteme sein. Es bleibt jedoch anzumerken, dass weder die beschriebenen Anwendungen noch das physikalische Netzwerk integraler Bestandteil der SuT Bw sind.

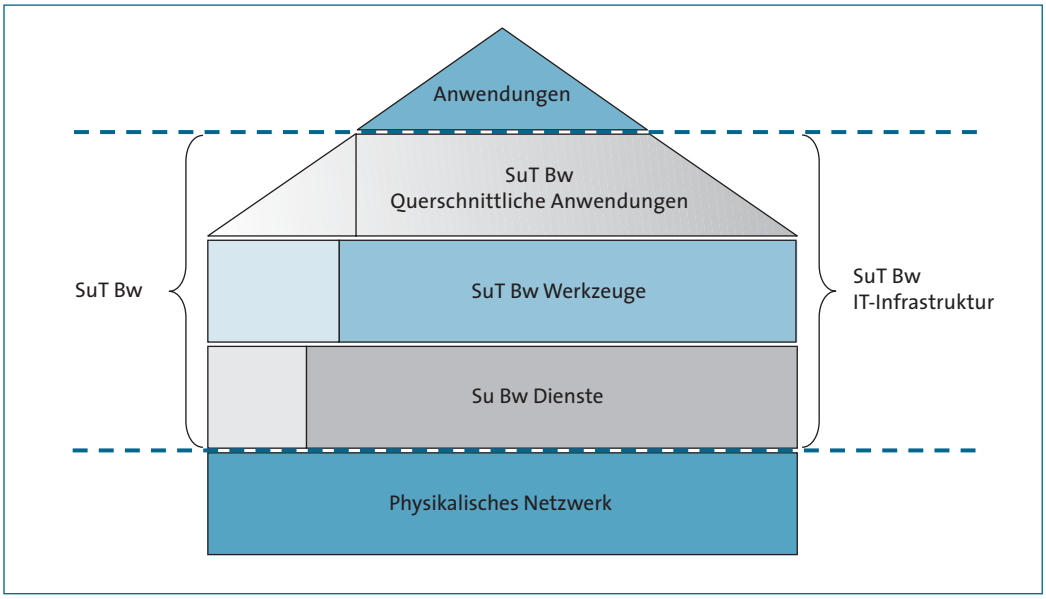


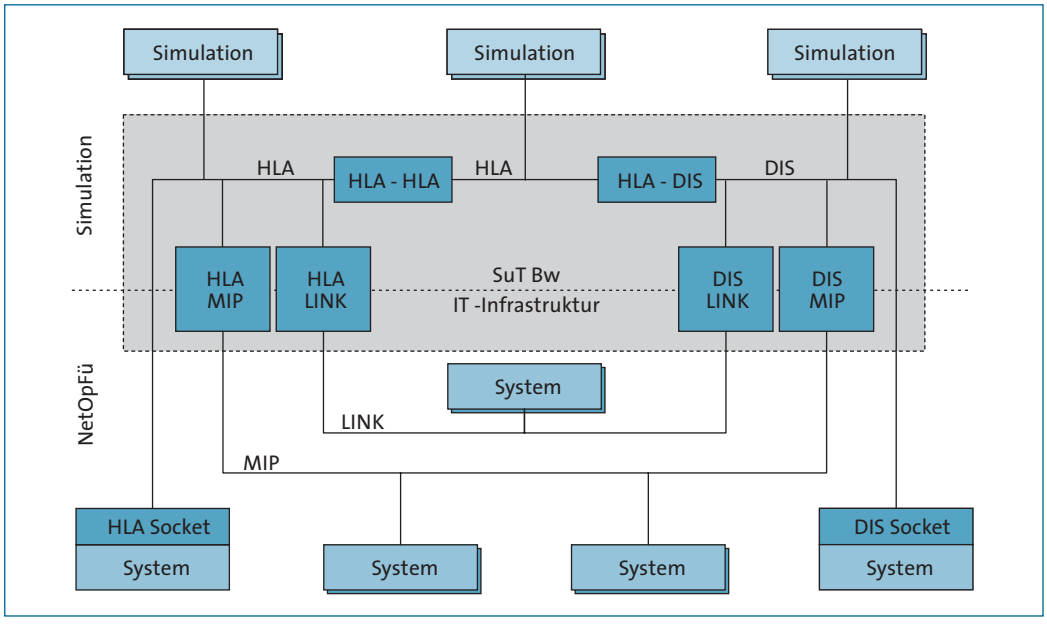
Abbildung 10: S&T als Drei-Ebenen-System

Die SuT Bw-Infrastruktur stellt Dienste und Werkzeuge zur Vorbereitung, Durchführung und Nachbereitung von Experimenten zur Verfügung. Die bereitgestellten Dienste ermöglichen die Anbindung von Anwendungen in einer Laufzeitumgebung. Sie sind modular aufgebaut und arbeiten, für den Anwender nicht sichtbar, im Hintergrund. Zu den wesentlichen Diensten zählt eine Middleware zur Anbindung einzelner Anwendungen an die oben angesprochene Laufzeitumgebung in verschiedenen Ausprägungen, sowie eine Vielzahl unterschiedlicher Datengateways, durch die die notwendige Flexibilität erreicht wird, um Experimentverbünde zu bilden. Die Werkzeuge der SuT Bw sind unabhängig von den Diensten einsetzbar und bilden unter anderem Funktionalitäten zur Konfiguration, Initialisierung, Steuerung und Überwachung von Experimentverbünden ab. Zu den wesentlichen Werkzeugen zählen:

S&T-Werkzeuge im Experimentverbund

- die Steuerungssoftware zum Management des Anwendungsverbunds; S&T-Werkzeuge im Experimentverbund;
- eine 2D/3D-Visualisierungssoftware;
- eine einheitliche Gelände- und Umweltdatenbasis;
- eine Datenaufzeichungs- und Analyseanlage;
- ein Wissensportal mit Kollaborationsfunktionalität;
- ein PC-Cluster mit Steuerungssoftware für simulationsgestützte Analysen.

Bei den in der obigen Abbildung dargestellten querschnittlichen Anwendungen handelt es sich um Systeme, die besonders häufig oder von mehreren Organisationsbereichen benötigt werden. Diese werden zentral, in der Regel als Software-Lizenzen zum Beispiel für Führungsinformationssysteme, über die SuT Bw zur Verfügung gestellt. Ihre Nutzung wird eng mit dem Nutzungsleiter abgestimmt. Die folgende Abbildung veranschaulicht den Einsatz der durch die SuT Bw bereitgestellten Datengateways im Kontext zur technischen Sicht der SuT Bw.



Abblidung 11: Datengateways bei NetOpFü und S&T (Quelle: Bundesamt für Informationsmanagement und Informationstechnik der Bundeswehr; angepasste Darstellung)

Mit geringem Adaptionsaufwand zum Erfolg

Die Realisierung der SuT Bw basiert auf einer Reihe von anwendungserprobten internationalen Standards. Dadurch wird die Interoperabilität mit unseren Partnern gewährleistet. Das Potenzial der Industrie für die zukünftige Nutzung der SuT ist hier sehr vielfältig. Neben den Fähigkeiten zur Planung, Analyse und Auswertung von Experimenten sind wiederkehrende Prozessabläufe zu definieren. Da innerhalb einer SuT Bw auch reale Systeme bzw. Systemanteile eingebracht werden sollen, ist die Erarbeitung von Systemschnittstelle ein wichtiges Gebiet für die Zusammenarbeit innerhalb der Industrie, aber auch mit dem öffentlichen Auftraggeber. Der Entwicklung dieser Systemschnittstellen auf der Basis von internationalen Standards kommt eine besondere Bedeutung zu.

S&T: Von zivilen Erfahrungen profitieren!

Nicht nur die Bundeswehr nutzt eine Simulations- und Testumgebung. Beinahe jeder Hersteller verfügt über industrielle Testbeds, die durch die klare Einhaltung von Standards an die SuT Bw angekoppelt werden können (Abbildung unten). Somit öffnet sich ein weites Feld für den Einsatz synthetischer Umgebungen bei der zukünftigen Entwicklung und Erprobung von Wehrmaterial. Die häufig schnell wechselnden Anforderungen der Einsatzkräfte im Ausland verlangen eine große Flexibilität bei der Umsetzung neuer Lösungen. Die Simulations- und Testumgebung bietet hierfür die richtigen Voraussetzungen. Neben der technischen Umsetzung werden Rahmenbedingungen und Verfahren entwickelt werden müssen, die eine optimale Nutzung der SuT Bw sicherstellen. Zum Beispiel ist eine unerlässliche Rahmenbedingung für die Durchführung von Experimenten die Entwicklung von entsprechenden Szenaren.

Auch nach Erreichung der so genannten Vollbefähigung wird die Weiterentwicklung der SuT Bw ein ständiger Prozess sein. Die Industrie kann und wird dazu einen maßgeblichen Beitrag leisten.

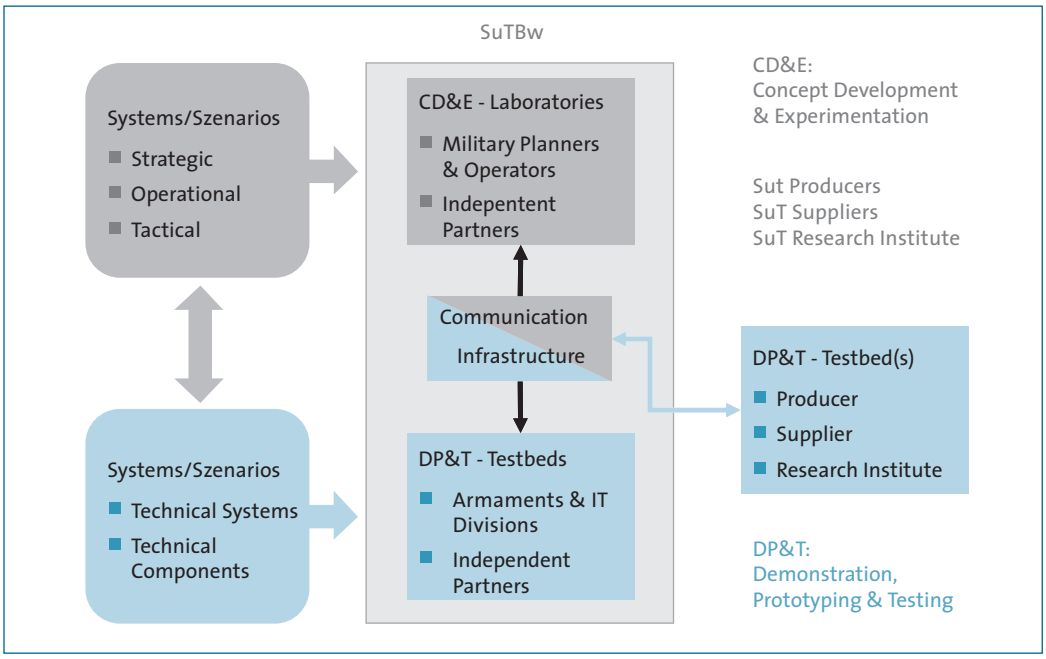


Abbildung 12: S&T im Zusammenhang

7 Verzeichnis der Abkürzungen und Fachbegriffe

Applicationlevel Gateway	Auch Proxy-Firewall genannt, bezeichnet einen Firewall-System-Typ
ASP	Application Service Providing
BPEL	Business Process Execution Language
CD&E	Concept Development and Experimentation
CERT	Computer Emergency Response Team
COMSEC	Communication Security (Kommunikationssicherheit)
Compute-Nodes	Frei übersetzt: Rechen-Knoten. Im Allgemeingebrauch Bezeichnung für einen einzelnen Rechner innerhalb eines Rechner-Verbundes.
Convertible Notebook	Notebook mit einem um 180° drehbaren Display – entweder als reguläres Notebook oder als Slate Tablet PC einsetzbar. Über Tastatur oder einen Stift bedienbar. Unterstützt die Handschriftenerkennung.
COTS	Commercial off the shelf, d. h. handelsübliche Produkte
EAI	Enterprise Application Integration
ERM	Enterprise Risk Management
ERP	Enterprise Resource Planning
Failover	Ungeplanter Wechsel von einem Primärserver zu einem zweiten Standby-System
GIS	Geoinformationssystem
IAM	Identity and Access Management
ISO / OSI Netzwerkmodell	Das Open Systems Interconnection Reference Model ist ein Schichtenmodel für die Kommunikation offener, informationsverarbeitender Systeme. Es wird seit 1979 entwickelt und ist von der ISO standardisiert
JSP	Java Server Pages
ITK	Informations- und Kommunikationstechnologien
LDAP	Lightweight Directory Access Protocol
Load Balancing	Lastverteilung
Mainframes	Großcomputer für Rechenzentren – zentralisierte Informationsverarbeitung. Ein Großrechner ist ein sehr komplexes und umfangreiches Computersystem, welches weit über die Kapazitäten eines Personal Computers, und oft über die der typischen Serversysteme hinaus geht. Ein Großrechner zeichnet sich vor allem durch seine Zuverlässigkeit und hohe Ein-Ausgabe-Leistung aus. Er kann im Online-Betrieb (Time Sharing) eine große Anzahl von Benutzern bedienen, im Batch-Betrieb aber auch komplizierte und aufwändige Aufgaben durchführen.
MIME-Types	Multimedia Internet Message Extentions
MOM	Message Oriented Models
NCW	Network-centric Warfare
NGN	Next Generation Network
NetOpFü	Netzwerkbasierte Operationsführung
OLAP	Online Analytical Processing

PDA	Ein Personal Digital Assistant (PDA) ist ein kleiner tragbarer Computer, der meist mit einem schnell startenden Betriebssystem ausgestattet ist und neben vielen anderen Programmen hauptsächlich für die persönliche Kalender-, Adress- und Aufgabenverwaltung benutzt wird. Derzeit werden die Geräte um weitere Anwendungen wie Navigation und Musik erweitert.
PKI	Public Key Infrastructure
Proxy	Proxy Representative (Stellvertreter) bezeichnet ein Dienstprogramm für Computernetze, das im Datenverkehr vermittelt
Racks	Wörtlich „Regale“ sind in der Regel Schränke für die Aufnahme unterschiedlicher Komponenten mit einer Einbaubreite von 19". In Racks werden Server, Storage, Netzwerkkomponenten, Stromversorgungen und andere technische Geräte eingebaut – oft in funktionaler Zusammenwirkung inkl. entsprechender Verkabelung. Standard 19“-Racks sind in unterschiedlichen Höhen, als Standard oder wassergekühlt verfügbar.
Servlet	Als Servlets bezeichnet man Java-Klassen, deren Instanzen innerhalb eines Webservers Anfragen von Clients entgegennehmen und beantworten.
SINA	Sichere Inter-Netzwerk Architektur
Slate Tablet PC	Mobiles Gerät, dessen Bauform eine fest integrierte Tastatur nicht vorsieht und damit Gewichtsvorteile mit sich bringt. Betriebssystem und Geräteausbau entsprechen einem herkömmlichen Notebook. Daten werden über das mit einer Sensorenmatte hinterlegte Display direkt mit Hilfe eines Pens handschriftlich eingegeben und im jeweiligen Programm digitalisiert.
SOA	Service Oriented Architecture
SOAP	Service Oriented Architecture Protocol, ehem. Simple Object Access Protocol
Storage	Bezeichnet in der IT allgemein „Datenspeicher“. Dies sind in der Regel Halbleiter-, Elektromagnetische- oder Optische Speichersysteme – abhängig vom jeweiligen Verwendungszweck. Beispiele: Hauptspeicher, Plattenspeicher, Bandspeicher, Optische Plattenspeicher, CD, DVD und andere.
Triple Play	Bündelangebot von Fernsehen, Sprachtelefonie und Internet
VPN	Virtual Private Network
WSDL	Web Services Definition Language
WSI	Web Services Integration
WVN	Wide Virtual Network

Der Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e.V. vertritt mehr als 1.000 Unternehmen, davon 800 Direktmitglieder mit etwa 120 Miliarden Euro Umsatz und 700.000 Beschäftigten. Hierzu zählen Geräte-Hersteller, Anbieter von Software, IT-Services, Telekommunikations-diensten und Content. Der BITKOM setzt sich insbesondere für bessere ordnungsrechtliche Rahmen-bedingungen, eine Modernisierung des Bildungssystems und eine innvationsorientierte Wirtschaftspolitik ein.

BITKOM
Connecting visions - creating solutions

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.
Albrechtstraße 10
10117 Berlin-Mitte

Tel: 030/27 576-0
Fax: 030/27 576-400

www.bitkom.org
bitkom@bitkom.org